ESTRATEGIAS DE GOBIERNO Y GESTIÓN DE TI PARA LAS CONTRALORÍAS TERRITORIALES CASO DEPARTAMENTO DE LA GUAJIRA.

Ing. HAMILTON MÁRQUEZ GULLOSO

Ing. DENIS CAROLINA VEGA MENDOZA

FUNDACIÓN UNIVERSIDAD DEL NORTE

DIVISIÓN DE INGENIERÍAS

MAESTRÍA GOBIERNO DE TECNOLOGÍA INFORMÁTICA

BARRANQUILLA – COLOMBIA

2017

ESTRATEGIAS DE GOBIERNO Y GESTIÓN DE TI PARA LAS CONTRALORÍAS TERRITORIALES CASO DEPARTAMENTO DE LA GUAJIRA.

Proyecto presentado como requisito para optar el titulo de Magíster en Gobierno de Tecnología Informática.

Ing. HAMILTON MÁRQUEZ GULLOSO

Ing. DENIS CAROLINA VEGA MENDOZA

DIRECTOR:

Ing. WILSON NIETO BERNAL Doctor en Ciencias de la computación ULPCG España

FUNDACIÓN UNIVERSIDAD DEL NORTE

DIVISIÓN DE INGENIERÍAS

MAESTRÍA GOBIERNO DE TECNOLOGÍA INFORMÁTICA

BARRANQUILLA – COLOMBIA

2017

Agradecimientos

En primer lugar, deseo dar gracias Dios, por darme la por darme la capacidad, y fortaleza para no desistir, y el entendimiento necesario para apropiar el valioso conocimiento que recibí.

De igual forma, deseo expresar mi profundo agradecimiento al director de este trabajo de grado el Doctor. Wilson Nieto Bernal, por el apoyo brindado, por la orientación y la paciencia en el desarrollo de este trabajo.

A la Contraloría General de Departamento de La Guajira por propiciar los espacios necesarios para realizar este proyecto.

Gracias a mi pareja por estar junto a mí en cada momento, a mi madre que con su ejemplo me enseñó a no desfaceller, a mi Padre que desde el cielo me ilumina con su presencia, y a mis hermanos porque con ellos comparto el esfuerzo de este logro.

Gracias a mis amigos, que siempre me han prestado un gran apoyo moral, profesional y humano, necesarios en los momentos difíciles, y en especial a Denis Vega Mendoza, quien me acompañó en esta aventura.

Ing. Hamilton Márquez Gulloso

Agradecimientos

A Dios por regalarme la oportunidad de cumplir este sueño.

Agradezco al profesor Wilson Nieto por ser mi guía en este proceso, a Hamilton Márquez Gulloso por ser mi compañero en este viaje.

A mi familia y amigos por su apoyo constante en cada momento especialmente a mi madre Denis Mendoza y a todos los que hoy no están pero desde el cielo cuidan mis pasos.

Ing. Denis Carolina Vega Mendoza

TABLA DE CONTENIDO

INTRODUCCIÓN **13**

1. DESCRIPCIÓN DEL PROBLEMA **16**

2. OBJETIVOS DEL PROYECTO **20**

2.1 OBJETIVO GENERAL **20**

2.2 OBJETIVOS ESPECÍFICOS **20**

3. METODOLOGÍA **21**

FASE 1. REVISIÓN DE LA LITERATURA Y ESTADO DEL ARTE. 21

FASE 2: PLANTEAMIENTO DEL MODELO DE REFERENCIA (FRAMEWORK). 21

FASE 3: IDENTIFICACIÓN DEL NIVEL DE MADUREZ ACTUAL Y NIVEL DESEADO. 21

FASE 4: PLAN DE IMPLEMENTACIÓN DEL FRAMEWORK PROPUESTO PARA LA CONTRALORÍA GENERAL CASO DEPARTAMENTO DE LA GUAJIRA. 22

4. MARCO TEÓRICO **23**

4.1 EL CAMBIO EVOLUTIVO DE TI EN LAS CONTRALORÍAS. **23**

4.2 Relación entre el Gobierno corporativo, empresarial y de TI. **24**

4.3 GOBIERNO CORPORATIVO. **25**

4.3.1 IMPORTANCIA Y OBJETIVOS DEL GOBIERNO CORPORATIVO. **26**

4.4 GOBIERNO DE TI. **27**

4.5 ALINEACIÓN ESTRATÉGICA DEL GOBIERNO DE TI Y EL GOBIERNO CORPORATIVO. **27**

4.6 Principales Desafíos de TI que deben enfrentar las Contralorías. **29**

4.7 PROPÓSITOs DEL GOBIERNO DE TI. **30**

4.8 EL ROL DEL CEO Y CIO **31**

4.9 Framework de Gobierno de TI Integrado 32
4.10 Áreas clave para el gobierno de TI 34
4.11 GESTIÓN DE LAS INICIATIVAS DE GOBIERNO DE TI. 35
4.12 Matriz toma de decisiones para Gobierno de TI en la Contraloría. 36
4.13 Direcciones, Comités, funciones y gobernanza de TI en la Contraloría. 37
4.14 MÉTRICAS y Modelo de madurez 39
5 MARCOS DE REFERENCIA 40
5.1 COBIT 5 40
5.1.1 PRINCIPIOS DE COBIT 5. 40
5.1.2 INTERACCIÓN ENTRE GOBIERNO Y GESTIÓN. 43
5.1.3 DOMINIOS Y PROCESOS DE COBIT 5. 44
5.2 NORMA ISO/IEC 27001:2013 46
5.3 NORMA ISO/IEC 27002:2013 47
5.4 ALINEACIÓN DE LOS PROCESOS DE COBIT 5.0 E ISO 27001:2013 EN TORNO A LA SEGURIDAD DE LA INFORMACIÓN 48
5.5 NORMA ISO 31000: GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES 53
6 MARCO REFERENCIAL 55
7 FRAMEWORK METODOLÓGICO PROPUESTO 62
7.1 GOBIERNO CORPORATIVO 62
7.2 GESTIÓN CORPORATIVA 64
7.3 GOBIERNO Y GESTIÓN DE TI 65
7.3.1 OBJETIVOS CORPORATIVOS Y DE TI 67
7.3.2 DOMINIOS 68
7.3.3 DETALLE DE PROCESOS DE TI 68
7.3.3.1 PLANEACIÓN Y DIRECCIÓN ESTRATÉGICA DE TI 68
7.3.3.2 GESTIÓN DE RIESGOS DE TI - RTI 70
7.3.3.3 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 71

7.3.3.4 GESTIÓN DE LA ARQUITECTURA EMPRESARIAL, ADQUISICIÓN Y SOPORTE DE TI 78
7.3.3.5 GESTIÓN DEL TALENTO HUMANO, APRENDIZAJE Y DESARROLLO - TAD 82
7.3.3.6 CONTROL, EVALUACIÓN Y MEJORA - CEM 84
7.4 ROLES Y RESPONSABILIDADES 85
7.5 INDICADORES DE DESEMPEÑO 92
8 MODELO DE MADUREZ 93
9 GUÍA DE IMPLEMENTACIÓN 94
Fase 1: Caracterización de la Entidad 95
Fase 2: Determinar el estado actual. 95
Fase 3: Establecer el estado futuro deseado e identificar las brechas. 96
Fase 4: Definir el plan de implementación 96
Fase 5: Ejecutar el Plan de Implementación 97
Fase 6: Medir y controlar el desempeño de la Implementación. 97
Fase 7: Supervisión, evaluación y mejora 98
10 CASO DE ESTUDIO: CONTRALORÍA GENERAL DEL DEPARTAMENTO DE LA GUAJIRA 99
10.1 CARACTERIZACIÓN 99
10.1.1 Misión 99
10.1.2 Visión 99
10.1.3 Estructura Organizacional 100
10.2 Estructura de procesos 100
10.2.1 SISTEMA INTEGRADO DE GESTIÓN DE CALIDAD 100
10.3 Historia 101
10.4 Productos y Servicios 103
10.5 Clientes 105
11 ESTADO ACTUAL 106

11.1 DOFA **106**
11.2 ESTADO ACTUAL Vs ESTADO DESEADO **108**
12 FUTURO DESEADO **110**
12.1 Estructura Organizacional Propuesta **111**
12.2 Modelo De Gobierno Y Gestión De Ti Propuesto, Aplicado A La Contraloría General Del Departamento De La Guajira **112**
12.3 Estructura de procesos del área de TI **113**
12.4 IDENTIFICACIÓN DE LAS BRECHAS **114**
13 PLAN DE IMPLEMENTACIÓN **117**
13.1 CRONOGRAMA 118
13.2 CARACTERIZACIÓN de los procesos 118
CONCLUSIONES Y RECOMENDACIONES **129**
REFERENCIAS BIBLIOGRÁFICAS **132**

LISTA DE FIGURAS

Figura 1: Modelo De Operación Por Procesos Contraloría De Boyacá. 17

Figura 2: Cambio Evolutivo De Ti En Las Contralorías. 23

Figura 3: Esencia Del Gobierno De TI. 28

Figura 4: Principales Desafíos De Ti En Las Contralorías. 29

Figura 5: Vinculación Del Ceo Con Las Iniciativas Empresariales. 32

Figura 6: Gestión De Iniciativas Desde Las Áreas Claves Del Gobierno De TI. 36

Figura 7: Direcciones Comités y Funciones de Gobernanza de TI. 38

Figura 8: Modelo De Madurez CMM. 39

Figura 9: Principios De COBIT 5. 40

Figura 10: Dominios Y Procesos De COBIT 5. 46

Figura 11: Dominios Y Objetivos De Control De La Norma ISO 27001: 2013. 48

Figura 12: Elementos De La Norma ISO 31000. 54

Figura 13: Modelo De G&G Corporativo Propuesto Para La Contraloría. 65

Figura 14: Modelo Propuesto De G&G De TI para La Contraloría. 66

Figura 15: Proceso guía de Implementación. 94

Figura 16: Estructura Organizacional de la CGDG 100

Figura 17: Mapa de Procesos CGDG. 101

Figura 18: Estructura Organizacional propuesta para la CGDG. 112

Figura 19: Modelo de Gobierno de Ti para la CGDG. 113

Figura 20: Estructura de procesos de Tecnología Informática para Contraloría Territoriales . 114

LISTA DE TABLAS

Tabla 1: Relación entre Gobierno Corporativo, Empresarial y de TI. 21

Tabla 2: Componentes y Prerrequisitos del framework integrado. 30

Tabla 3: Matriz toma de decisiones para el Gobierno de TI. 33

Tabla 4: Interacciones entre gobierno y gestión en COBIT 5. 39

Tabla 5: Mapeo de procesos COBIT 5 e ISO 27001: 2013. 46

Tabla 6: Objetivos corporativos y de TI. 63

Tabla 7: Escala de Medición de procesos según ISO 15504. 89

Tabla 8: Medición nivel de madurez por Procesos. 104

Tabla 9: Medición Nivel de Madurez por Dominios. 112

LISTA DE GRÁFICOS

Grafico 1: Nivel de Madurez por Procesos. 107

Grafico 2: Nivel de Madurez por dominio: 113

LISTA DE ANEXOS

Anexo 1: Ficha Técnica Encuesta Gobierno Y Gestión De Ti- Contralorías Territoriales.

Anexo 2: Respuestas Encuesta Gobierno y Gestión de TI, Contralorías Territoriales.

Anexo 3: Gráficos de Consolidados de Respuestas.

INTRODUCCIÓN

Las tecnologías de la información (TI), constituyen una importante herramienta de apoyo en la gestión administrativa de las empresas tanto públicas como privadas, cada vez más las organizaciones están dependiendo de sus sistemas de información como apoyo para la toma de decisiones, la coordinación, el control (Laudon & Laudon, 1996), y el desarrollo de nuevos productos o servicios, entre otros procesos.

De igual forma, la globalización, la competencia, la eficiencia administrativa y demás factores, han hecho que la información se convierta en un elemento clave para la gestión de las empresas, y determina un factor de supervivencia y crecimiento de las mismas(Trasobares, 2003).

Conforme a lo anterior, es importante resaltar que en el marco del gobierno corporativo, la gestión estratégica debe permitir dirigir, administrar, monitorear y evaluar los procesos de TI, de forma tal que al ser alineados con los objetivos del negocio, promuevan el crecimiento y posicionamiento del mismo, teniendo como referencia el entorno competitivo y la búsqueda de beneficios económicos y/o sociales, según sea el caso (Selig G, 2010).

En Colombia, las grandes, medianas y pequeñas empresas, también buscan estar a la par de las grandes potencias en el tema de TI, procurando la productividad y competitividad de sus organizaciones, teniendo en cuenta que la información y la tecnología que la soporta representan los activos más valiosos de las mismas, para lo cual muchos están basando sus procesos en sistemas de información que les ayudan a fortalecer su gestión estratégica y alcance en el mercado.

En referencia a las entidades públicas, la estrategia gobierno en Línea (GEL), liderada por el gobierno nacional de Colombia, ha hecho ingentes esfuerzos para fortalecer la gestión de TI en las entidades de orden nacional y territorial, buscando el

acercamiento con la ciudadanía y la mejora en la prestación de los servicios, maximizando el beneficio social (Mintic, 2015).

La adopción de esta estrategia por parte de las entidades públicas, pretende un cambio en el modelo de operación de las mismas, buscando ofrecer más y mejores servicios a la comunidad, utilizando como herramienta las tecnologías de la información y la comunicación, incluyendo dentro de sus estructuras organizativas el área de TI, en el nivel directivo y no solamente como apoyo a la gestión administrativa.

Uno de los componentes de la estrategia GEL, hace referencia a la planeación y gestión tecnológica, la mejora de procesos internos y el intercambio de información. Igualmente, la gestión y aprovechamiento de la información para el análisis, toma de decisiones y el mejoramiento permanente, con un enfoque integral para una respuesta articulada de gobierno y hacer más eficaz la gestión administrativa (**TIC para la Gestión)**

De igual forma, se hace referencia dentro de esta estrategia, al componente de **Seguridad y Privacidad de la Información**, el cual comprende las acciones tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada.(Mintic, 2015)

En el presente trabajo, se analizara la situación actual de las contralorías territoriales, como sujetos obligados por la normatividad vigente en la implementación de la estrategia gobierno en línea, específicamente en los componentes de TIC para la gestión, representado a través de un esquema de Gobierno de TI y la gestión de la seguridad de la información, para lo cual se realizará una indagación previa en las contralorías territoriales sobre el conocimiento de estos tema y el estado actual de implementación de los mismos.

De la misma forma, se determina un modelo de Gobierno y Gestión de TI que puede ser aplicado a las contralorías territoriales, como herramienta de apoyo para la optimización de los procesos de TI, el cumplimiento de la normatividad, procurando la

eficiencia administrativa, basado en las mejores prácticas que ofrecen los diferentes marcos de referencia como lo son COBIT 5 e ISO 27001 en su revisión del 2013, y la guía de administración del riesgo definida en la norma ISO 31000, para ello se hace una revisión genérica de la literatura y estado del arte para la construcción del marco teórico y referencial que argumenta y sustenta el framework propuesto para el buen gobierno y gestión de TI.

Seguidamente, se propone una guía de implementación del Modelo de Gobierno y Gestión planteado, tomando como referencia o caso de estudio la Contraloría General del Departamento de La Guajira, haciendo una medición del nivel de madurez de los procesos de TI definidos en el Framework de G&G que se propone, para de esta forma determinar un Plan de Implementación de los mismos teniendo como punto de partida esta medición, dicho plan está encaminado a lograr los objetivos corporativos y de TI, en relación a la Seguridad y privacidad de la Información, y por último, se plasman las conclusiones derivadas del este trabajo y se plantean recomendaciones para la correcta ejecución del plan de implementación propuesto.

1. DESCRIPCIÓN DEL PROBLEMA

El desarrollo del Framework propuesto para el buen gobierno y gestión de TI toma como referente las contralorías territoriales de la República de Colombia, organismos de carácter técnico dotadas de autonomía administrativa, presupuestal y contractual, la cual ejerce la función pública de control fiscal en su respectiva jurisdicción (Departamento, Municipio o Distrito), de acuerdo con los principios, sistemas y procedimientos establecidos en la Constitución y la ley, cuya función principal es vigilar la gestión fiscal de la administración y de los particulares o entidades que manejen fondos o bienes de la Nación.

Actualmente existen 63 Contralorías territoriales de las cuales 32 son de orden Departamental, 4 distritales y 26 municipales, para el caso, se tomo una muestra de 29 contralorías (11 Departamentales, 17 Municipales, 1 Distrital,, con el fin de obtener la información directamente, a dichas entidades se les realizó una consulta relacionada con el tema de estudio (Gobierno y gestión de TI – Anexo 1), por medio de una encuesta en línea, cuyos resultados indican que 17 de estas entidades cuentan con un área de gestión de TI, sin embargo, tan solo una de ellas (la Contraloría de Boyacá), la ubica en el nivel estratégico, este hecho se puede corroborar en su mapa de procesos (Figura 1).

Figura 1: Modelo de Operación por Proceso, Contraloría de Boyacá
Fuente: Contraloría de Boyacá.

No obstante lo anterior, esta entidad y ninguna de las consultadas, no tienen definido un esquema de Gobierno TI alineado con la estrategia misional y con el Modelo Integrado de Planeación y Gestión, que estructure y direccione el flujo de las decisiones de TI, también se observa que solo 9 de las 29 entidades consultadas tienen definido el Plan Estratégico de TI, sin embargo, 21 de estas indicaron que tienen adoptados políticas y estándares relacionados de seguridad de la información y privacidad de la información, lo que denota que los mismos no están alineados con la planeación estratégica de TI.

En relación al gobierno y gestión de las TI en las contralorías territoriales, es preciso mencionar que estas entidades son destinatarias y sujetos obligados de la implementación de la estrategia Gobierno en Línea, reglamentada por la el decreto 2573 de 2014 y contenido en el Decreto Único Reglamentario 1078 de 2015, liderada por el gobierno nacional de Colombia, ha hecho ingentes esfuerzos para fortalecer la

gestión de TI en las entidades de orden nacional y territorial, buscando el acercamiento con la ciudadanía y la mejora en la prestación de los servicios, maximizando el beneficio social.

La adopción de esta estrategia por parte de las entidades públicas, pretende un cambio en el modelo de operación de las mismas, buscando ofrecer más y mejores servicios a la comunidad, utilizando como herramienta las tecnologías de la información y la comunicación, incluyendo dentro de sus estructuras organizativas el área de TI, en el nivel directivo y no solamente como apoyo a la gestión administrativa, además se incluye dentro de sus componentes, la definición de una estructura de gobierno de TI alineada a la plataforma estratégica de las entidades y la gestión de la seguridad de la información.

El informe de la estrategia gobierno en línea, publicado en el año 2016, mide los avances de la implementación en los niveles nacional y territorial, dentro de estos últimos, las contralorías territoriales, muestra que estas entidades solo han implementado la estrategia en un 45.17%, lo que significa una deficiente apropiación de la estrategia, según lo requerido por el Ministerio TIC.

Lo anterior es una situación crítica, que puede traer repercusiones de tipo legal, teniendo presente que el gobierno nacional de Colombia ha emitido normativas asociadas al tema, las cuales son de carácter vinculatorio para todos los entes públicos nacionales y territoriales, como es el caso de la estrategia gobierno en línea y el decreto 415 de 2016, mediante el cual se definen los lineamientos para el fortalecimiento institucional en materia de tecnologías de la Información y las comunicaciones.

De igual forma, la inexistencia de una estrategia de Gobierno y Gestión de TI, incide en la deficiente planeación estratégica relacionada con las inversiones, que en materia de nuevas tecnologías de la información y la comunicación, permiten aprovechar la evolución de las mismas para el buen desarrollo de los procesos

misionales (Control fiscal, Responsabilidad fiscal, Participación Ciudadana),e incluso el acercamiento con la comunidad, lo que impacta de forma negativa en la percepción de la ciudadanía hacia la labor de vigilancia y control realizadas.

Por otra parte, en estas entidades se produce un alto volumen de información que requiere un manejo apropiado que asegure la confidencialidad, disponibilidad,e integridad de la misma, por lo que cual es importante contar con un Sistema de Gestión de Seguridad de la Información, que desde el nivel directivo, se gestione, administre y defina las políticas de custodia de la misma, con el fin de no exponerse a altos riesgos de vulnerabilidad en materia de seguridad informática e ineficiencia administrativa, debido a la falta de control de entradas y salidas, duplicidad de datos, y repercusiones de tipo legal con respecto a las normativas aplicables a la privacidad y seguridad de la información que se genera.

Lo anterior pone de manifiesto la necesidad de un modelo de Gobierno y gestión de TI, que permita suplir las falencias detectadas anteriormente, establezca una adecuada gestión de la inversión, infraestructura y servicios informáticos con los que cuenta, además que determine los procesos y controles requeridos para la gestión de la seguridad de la información.

Teniendo en cuenta lo expuesto se buscará dar respuesta a la pregunta: ¿Cuál debe ser el modelo de Gobierno y Gestión necesario para el aprovechamiento de las Tecnologías de la Información y la Comunicación, y la seguridad y privacidad de la información, aplicable a las Contralorías Territoriales?

2. OBJETIVOS DEL PROYECTO

2.1 OBJETIVO GENERAL

- ❏ Diseñar un framework que proporcione estrategias de gobierno, gestión de TI y seguridad de la información que sirva como referencia para las contralorías territoriales, basándonos en el mapeo de los procesos de las mejores prácticas COBIT 5, ISO/IEC 27001: 2013 e ISO/IEC 31000.

2.2 OBJETIVOS ESPECÍFICOS

- Realizar de una revisión genérica de la literatura y estado del arte para la construcción del marco teórico y referencial que argumenta y sustenta el framework propuesto para el buen gobierno y gestión de TI.
- Generar un mapeo de los procesos de las mejores prácticas COBIT 5 e ISO/IEC 27001 ajustables al framework propuesto para gestionar la seguridad de la información de la contraloría general caso departamento de la Guajira.
- Adoptar el proceso de gestión Riesgos basado en la Norma ISO/IEC 31000, que sean propicios para la identificación, valoración y tratamiento de los riesgos asociados a TI, transversal a toda la organización.
- Identificar el nivel de madurez actual Vs nivel de madurez deseado de la contraloría general caso departamento de La Guajira en cuanto a gobierno, gestión y seguridad de la información.
- Proponer un plan de implementación de estrategias de gobierno, gestión de TI y seguridad de la información para la contraloría general caso departamento de La Guajira.

3. METODOLOGÍA

FASE 1. REVISIÓN DE LA LITERATURA Y ESTADO DEL ARTE.

En esta fase se realizará una revisión genérica de la literatura existente y del estado del arte actual sobre la temática de gobierno y gestión de TI y seguridad de la información haciendo énfasis en el framework COBIT 5 y NORMA ISO 27001 del 2013. Esto permitirá construir el marco teórico conceptual y el marco referencial que va a soportar, argumentar y sustentar la propuesta de gobierno y gestión de TI para la contraloría general caso departamento de la Guajira, además puede servir de referente para investigaciones o trabajo similares que se realicen posteriormente.

FASE 2: PLANTEAMIENTO DEL MODELO DE REFERENCIA (FRAMEWORK).

En esta fase se identificarán los dominios de COBIT 5 y se seleccionarán los que más se ajusten de acuerdo a la necesidad para la construcción del framework para el buen gobierno y la gestión de TI para la contraloría general caso departamento de la Guajira, de la misma se identificarán y alinearán los requisitos de la norma ISO/IEC 27001 que sean ajustables al sistema de gestión para la seguridad de la información de las contralorías territoriales, para ser aplicado a la Contraloría del departamento de la Guajira, y se adoptaran los procesos establecidos en la Norma ISO/IEC 31000, para la gestión de Riesgos de TI.

FASE 3: IDENTIFICACIÓN DEL NIVEL DE MADUREZ ACTUAL Y NIVEL DESEADO.

En esta fase se identifica el nivel de madurez actual de los procesos de la contraloría general del departamento de la Guajira usando la escala de valoración de la norma ISO 15504, obteniendo como resultado el nivel de madurez inicial y el deseado, con este resultado permite proponer estrategias de gobierno y gestión para disminuir las brechas existentes.

FASE 4: PLAN DE IMPLEMENTACIÓN DEL FRAMEWORK PROPUESTO PARA LA CONTRALORÍA GENERAL CASO DEPARTAMENTO DE LA GUAJIRA.

A partir de las estrategias diseñadas para disminuir las brechas se propone un plan de implementación del framework de gobierno, gestión de TI y seguridad de la información para la Contraloría General del Departamento de la Guajira, que de igual forma sea aplicable para otras entidades de control fiscal de orden territorial.

4. MARCO TEÓRICO

4.1 EL CAMBIO EVOLUTIVO DE TI EN LAS CONTRALORÍAS.

La figura 2, ilustra las presiones y tendencias que las contralorías deben hacer frente en un entorno global que cambia rápidamente y de forma dinámica como: la innovación, cumplimientos de leyes y regulaciones, rendición de cuentas más eficaz, la globalización, tecnologías más sofisticadas etc., las contralorías funcionan en un entorno global que cambia rápidamente y de forma dinámica debido al constante cambio evolutivo de las tecnologías de la información, a continuación se hace una adaptación aplicada al caso de estudio de este proyecto que son las contralorías territoriales.

Figura 2: Cambio evolutivo de TI en las Contralorías
Fuente: Adaptado de Selig G, Implementing IT Governance, 2010.

4.2 RELACIÓN ENTRE EL GOBIERNO CORPORATIVO, EMPRESARIAL Y DE TI.

Según la Federación Internacional de Contadores (IFAC), "*Gobierno empresarial constituye el marco de rendición de cuentas de la organización*"

El Gobierno corporativo es el conjunto de responsabilidades, reglas y practicas ejercidas por la Junta ejecutiva y la alta dirección, con el objetivo de proporcionar direccionamiento estratégico, asegurándose que se cumplan todos los planes y objetivos, la evaluación, gestión de riesgos de forma proactiva y asegurar que los recursos de la empresa se utilizan de forma responsable, en este sentido el Gobierno Corporativo se encarga de la separación de la propiedad y el control de una organización, mientras que el gobierno empresarial se centra en la dirección y control de la empresa, y el gobierno de TI se centra en la dirección y control de las tecnologías de la información. (Selig, 2010).

Como entes autónomos, en las contralorías territoriales el modelo corporativo está en cabeza del contralor territorial como ente máximo de la organización, el mismo es el encargado de proporcionar el direccionamiento estratégico de la entidad, por su parte los funcionarios de nivel directivo son los encargados de que se cumplan los planes y objetivos corporativos, la evaluación y gestión de riesgos y asegurar que los recursos de la empresa se utilicen de forma responsable.

Gobierno Corporativo	Gobierno Empresarial	Gobierno de TI
Separación de propiedad y control de la empresa	**Dirección y control de la empresa.**	**Dirección y control de TI.**
Cumplimiento normativo (Leyes, Regulaciones).	Estrategia de productos y servicios.	Estrategia de TI.
Rendición de cuentas.	Planes y Objetivos	Alineación de los objetivos de TI con los de la empresa.
Gestión de riesgos	Procesos y actividades empresariales	Administración de recursos de TI.
	Innovación e Investigación	Servicio de Gobierno en Línea.
	Capital intelectual	Entrega y Ejecución de Valor Agregado para garantizar la continuidad de la empresa)
	Gestión de RH.	Gestión de proyectos de TI.
	Métricas de rendimiento y controles.	Administración de riesgo y seguridad de la información.
	Gestión de activos	

Tabla 1. Relación entre el Gobierno corporativo, empresarial y de TI.
Fuente. Adaptado de Implementing IT Governance, (Selig G, 2010)

4.3 GOBIERNO CORPORATIVO.

El Gobierno Corporativo En el Documento conceptual de gobierno corporativo, de la Superfinanciera, se define el gobierno corporativo como: "(…) sistema (conjunto de normas y órganos internos) mediante el cual se dirige y controla la gestión de una persona jurídica, (...) provee un marco que define derechos y responsabilidades, dentro del cual interactúan los órganos de gobierno de una entidad entre los que se destacan el máximo órgano de dirección, la junta o consejo directivo, los representantes legales y

demás administradores, el revisor fiscal y los correspondientes órganos de control" (Superintendencia financiera de Colombia, 2010).

Teniendo en cuenta lo anterior, sumado a lo conversado en la OCDE sobre los principios de gobierno corporativo, podemos decir que comprende las acciones administrativas y de gerencia organizacional, que interrelaciona a todas las partes interesadas de la empresa (consejo de administración, accionistas y demás órganos de gobierno), desde el cual se traza los lineamientos y objetivos corporativos, y se determina la estrategia a seguir para alcanzar dichos objetivos.(Organización para la Cooperación y el Desarrollo Económico(OCDE), 2004).

4.3.1 IMPORTANCIA Y OBJETIVOS DEL GOBIERNO CORPORATIVO.

Según el Banco Mundial los siguientes aspectos son los beneficios del gobierno corporativo.

Mayor acceso al financiamiento.

Mayor valoración de las empresas.

Mejor desempeño operacional.

Menor riesgo de crisis financieras.

Mejores relaciones con otras partes interesadas.

Por su parte, en el reporte Hampel, se señala lo siguiente: "La importancia del gobierno corporativo reside en su contribución a la prosperidad de las empresas y a la rendición de cuentas. (…) El buen gobierno vela por que aquellos grupos (partes interesadas) con un interés pertinente en las actividades de la empresa sean tenidos en cuenta plenamente". (Williams, 1998).

4.4 GOBIERNO DE TI.

El gobierno de TI es el centro de coordinación para la gestión de TI más eficaz, alrededor de la cual hay muchos temas importantes, como la alineación, el liderazgo, la planificación, la ejecución, la rendición de cuentas, la gestión del cambio, los indicadores clave de rendimiento y temas relacionados. Gad J Selig (2016).

Según David Norfolk gobierno de TI hace parte de la gestión empresarial en general, lo que asegura que sistemas automatizados contribuyen eficazmente a la consecución de los objetivos de una organización identificando y gestionando adecuadamente los riesgos relacionados con TI y garantizando que los sistemas de información automatizados incluyendo sistemas de información financiera y de auditoría proporcionan una imagen real de la operación de la empresa.

En este sentido, el gobierno de TI facilita que la empresa aproveche al máximo su información, maximice sus beneficios, canalice las oportunidades y gane ventajas competitivas. Tomado de: COBIT: Un marco de referencia para la información y la tecnología. (BITCompany, 2015)

4.5 ALINEACIÓN ESTRATÉGICA DEL GOBIERNO DE TI Y EL GOBIERNO CORPORATIVO.

El gobierno de TI garantiza que los objetivos de TI estén alineados con la estrategia de la empresa y le permite administrar sus recursos, gestionar los riesgos, la seguridad de la información y además Del desempeño de sus recursos para generar valor agregado a la empresa.

De acuerdo con Luftman, Papp y Brier, “El logro de alineación es evolutiva y dinámica. Se requiere un fuerte apoyo de la alta dirección, buenas relaciones de trabajo, un fuerte liderazgo, la priorización adecuada, la confianza y la comunicación efectiva, así como conocimiento profundo del entorno empresarial” (Luftman, Papp y Brier, 1999).

Figura 3. Esencia del Gobierno de TI.
Fuente: http://www.bitcompany.biz/wp-content/uploads/2012/04/que-es-cobit.jpg

De lo anterior, se desprende que la esencia del Gobierno de TI la constituyen generar valor agregado al negocio, la gestión del riesgo y el control, lo cual se puede entender mediante la interpretación de la Figura 1.

La alineación estratégica entre los objetivos del negocio y los de TI son una necesidad y un reto que toda entidad debe asumir y las entidades de control como los son las contralorías no son la excepción por lo que es necesario alinear de forma estratégica los objetivos de la contraloría con los objetivos de TI de dicha entidad teniendo presente la evolución tecnológica y asumiendo que TI pasó de ser una herramienta de trabajo a ser un componente valioso sin el cual cualquier entidad puede fracasar.

Consecuentemente a esto es inevitable asumir un enfoque integral que contenga todas las actividades necesarias para lograr un alineamiento de TI con el negocio como lo son: planificación, puesta en marcha del gobierno de TI, asimismo como el liderazgo de los autorizados de la operación, todo esto es fundamental para lograr un solución

efectiva en el uso de tecnologías más cuando somos proveedores de productos o servicios.

4.6 PRINCIPALES DESAFÍOS DE TI QUE DEBEN ENFRENTAR LAS CONTRALORÍAS.

Los principales desafíos y retos que deben ser tratados como parte de la planificación de procesos de Gobierno de TI para adoptar o implementar un marco de Gobierno y gestión de TI Las Contralorías deben enfrentarse a una serie de desafíos de los cuales deben identificar los más importantes para enfrentarlos sacando provecho y ventajas de estos, ya que los desafíos considerados como principales se deben incorporarse en la Gestión de TI y por lo tanto se les debe hacer un tratamiento como parte del proceso de planificación y gobernanza.

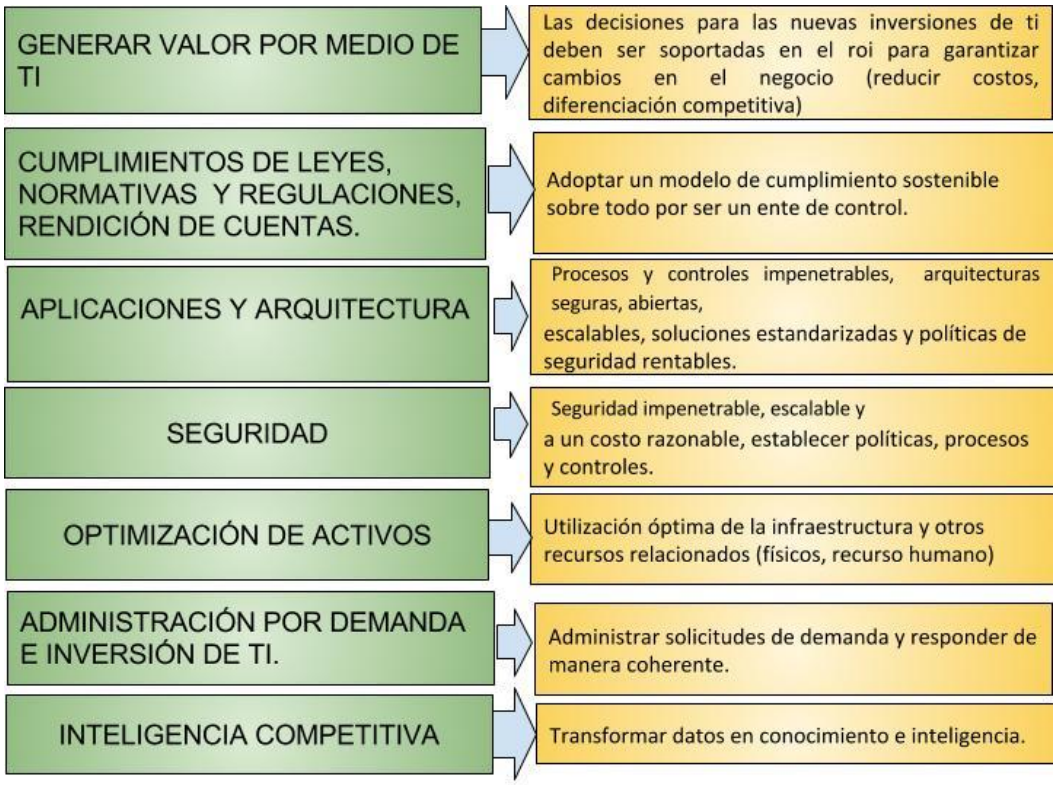


Figura 4: Principales Desafíos de TI en las Contralorías.
Fuente**:** Adaptado de Selig G, Implementing IT Governance, 2010.

4.7 PROPÓSITOS DEL GOBIERNO DE TI.

- ✓ Alinea las inversiones y prioridades de TI más estrechamente con el negocio
- ✓ Gestiona, evalúa prioriza, fondos, medidas y supervisa las solicitudes y servicios de TI, y el trabajo y productos resultantes, de una manera más consistente y repetible que optimiza los rendimientos de la empresa y retorno del valor.
- ✓ Mantiene la utilización responsable de los recursos y activos
- ✓ Define claramente las autoridades, roles funciones, responsabilidades en los procesos que competen a TI.
- ✓ Asegura que cumple con sus planes, presupuestos y compromisos.
- ✓ Gestiona los principales riesgos, las amenazas, el cambio y contingencias de forma proactiva.
- ✓ Mejora el rendimiento de TI de la organización, el cumplimiento, la madurez, el desarrollo del personal y la externalización de las iniciativas.
- ✓ Mejora la gestión de la demanda y en general y satisfacción del cliente constituyente y capacidad de respuesta
- ✓ Gestiona y piensa globalmente, pero actúa localmente
- ✓ Gestionar la innovación continua.

El caso de estudio de este proyecto la Contraloría territorial del Departamento de la Guajira, es necesario garantizar trasparencia, eficacia y eficiencia en la prestación de sus servicios, seguridad de la información y gestión del riesgo, para ello debe

adaptarse rápidamente al entorno cambiante contar con la tecnología adecuada además de la adopción de la mejores prácticas que garanticen una adecuada administración de la misma. Selig (2010).

Los resultados y consecuencias de un ineficaz Gobierno de TI pueden ser devastadores.

- ✓ Pérdidas e interrupciones de negocios, daño en la reputación y posiciones competitivas debilitadas.
- ✓ Horarios no cumplidos, mayores costos, mala calidad en la prestación de servicios y clientes insatisfechos.
- ✓ Los procesos básicos del negocio se ven afectados negativamente lo que impide el cumplimiento de leyes y regulaciones externas.
- ✓ Falla de TI para demostrar sus beneficios de inversión o propuestas de valor.

4.8 EL ROL DEL CEO Y CIO

El rol del Contralor (CEO) requiere equilibrio entre mantener el crecimiento y continuidad de la contraloría al tiempo que optimiza la eficacia organizativa y ayuda a cumplir con la creciente serie de requisitos regulatorios. Selig G, 2010.

Figura 5: Vinculación del CEO con las iniciativas empresariales.

Fuente: adaptado de Selig G, Implementing IT Governance, 2010

4.9 FRAMEWORK DE GOBIERNO DE TI INTEGRADO

El Marco de gobierno integrado consiste en cinco componentes críticos del Gobierno de TI y abordan las siguientes áreas de trabajo:

Estrategia Empresarial, el plan y los objetivos (gestión de la demanda): esto implica el desarrollo de la estrategia y el plan de negocio que deben impulsar la estrategia y el plan de TI, la estrategia empresarial está definida (Misión, Visión, valores, etc.), además del Plan de Gobierno de cada Contralor, si existe un gobierno de TI, donde el CIO pueda estar en la junta directiva, se tendrá la oportunidad de proponer

estrategias en el plan de Gobierno Institucional a favor del plan de TI buscando alinear los objetivos de Ti con la estrategia del negocio.

Estrategia, Plan y Objetivos de TI, está basado en el plan estratégico y objetivos de la entidad, y proporciona a la dirección un informe con las prioridades de las funciones de TI y recursos; Inversiones de cartera, prioridad e identificar los derechos de decisión (quién influye en las decisiones y quién está autorizado para tomar las decisiones) en una amplia variedad de áreas de TI; Además, el CIO es responsable de las inversiones en infraestructura tales como servidores, redes, software de administración, Al implementar estrategias, planes y objetivos, en el área de TI en la Contraloría, el CIO podrá priorizar las inversiones y responder a las exigencias de la Alta Dirección, esto brindará agilidad en los procesos de adquisición y habilitación de tecnología que apalanquen la estrategia de la entidad.

Ejecución del plan de TI, abarca los procesos de gestión de proyectos y gestión de servicios de TI (incluyendo COBIT 5, ISO 27001, Gestión de riesgos, gestión del cambio, gestión de la continuidad del negocio etc.

Gestión del rendimiento y controles de gestión; incluye el Balanced Scorecard, indicadores clave de desempeño, COBIT 5 y áreas de cumplimiento normativos leyes y regulaciones.

El desarrollo del talento humano, la mejora continua de los procesos y el aprendizaje; Invertir en el TH, la gestión del conocimiento y sostener la mejora continua iniciativas de innovación.

Para cada componente de gobierno de TI, el primer paso para un nuevo CIO es evaluar el medio ambiente y la forma en la que se encuentra.

Para el caso de estudio de Este proyecto que son las Contralorías proponemos un framework de Gobierno y Gestión de TI, que nos permita alinear los objetivos de TI con la estrategia de la entidad. Para esto es necesario identificar cuáles son las áreas

de trabajo claves y sus respectivos componentes y entregables o referencias, de esta forma lograremos la integración de ambos lineamientos.

ÁREA DE TRABAJO	COMPONENTES	ENTREGABLES / REFERENCIAS
Alineación de los objetivos de TI con la estrategia de la Contraloría.	-Plan Estratégico. -Identificar debilidades, oportunidades, fortalezas y amenazas(DOFA), -Planificación de Gastos e inversiones de TI. - Métricas del BSC. - Evaluación de la gestión (Rendición de cuentas). - Gestión del desempeño de TI (métricas e indicadores).	-Documento del plan Estratégico Contraloría. - Plan estratégico de TI.
Gestión de la ejecución y recursos.	- Plan operativo de TI. - Políticas, estándares y lineamientos. - Seguridad de la información.	- Roles y responsabilidades. - Plan de infraestructura y operaciones. - Seguridad de la información (ISO 27001) - COBIT 5.
Administración del desempeño, Controles, Riesgos.	-Definición y aseguramiento de indicadores claves de desempeño. - Plan de continuidad del negocio. -Políticas, Estándares, -Seguridad -Gestión del Riesgo.	- BSC Y KPIs (indicadores claves de rendimiento). - Rendición de cuentas. -Métricas. - COBIT 5. -ISO 27001 Gestión de Seguridad de la información. -Nivel de madurez actual y nivel de madurez deseado. -Plan de Continuidad
- Desarrollo de personas, Mejora continua de procesos y aprendizaje	- Formación del TH. - Gestión del cambio. -Formación y certificación. -Gestión del cambio y la transparencia.	- Administración de contratos - Plan de carreras y certificaciones. -Gobierno en línea. - Adopción de las Mejores prácticas y estándares.

Tabla 2: Componentes y prerrequisitos del framework integrado.
Fuente: Adaptado de Selig G, Implementing IT Governance, 2010.

4.10 ÁREAS CLAVE PARA EL GOBIERNO DE TI

La implementación del Gobierno de TI dentro del contexto de las Contralorías permite la distribución de paquetes de trabajo que puedan ser asignados y verificados,

el talento humano es clave en este proceso para el desarrollo y mejoramiento continuo, las áreas principales de trabajo para el gobierno de TI son:

Gestión de la planeación: Asegurar el desarrollo de estrategias y planes operativos de alta calidad.

Gestión de la ejecución: emprender proyectos definidos y asegurar que sean completados en el tiempo y presupuesto estimados.

Gestión del desempeño: definir indicadores claves de medición para cada función. Establecer metas y monitorear el rendimiento, utilizando BSC.

Gestión de la creación de valor: asegurar que los servicios, gestión y entrega de TI se encuentran documentados y que los indicadores claves de rendimiento son medidos para asegurar los niveles de servicio apropiados para la entidad.

4.11 GESTIÓN DE LAS INICIATIVAS DE GOBIERNO DE TI.

Según Selig G, 2010.La Iniciativa de Gobierno de TI debe ser descompuesta en paquetes de trabajos administrables y asignados a los propietarios para la planificación, desarrollo, ejecución y mejora continua.

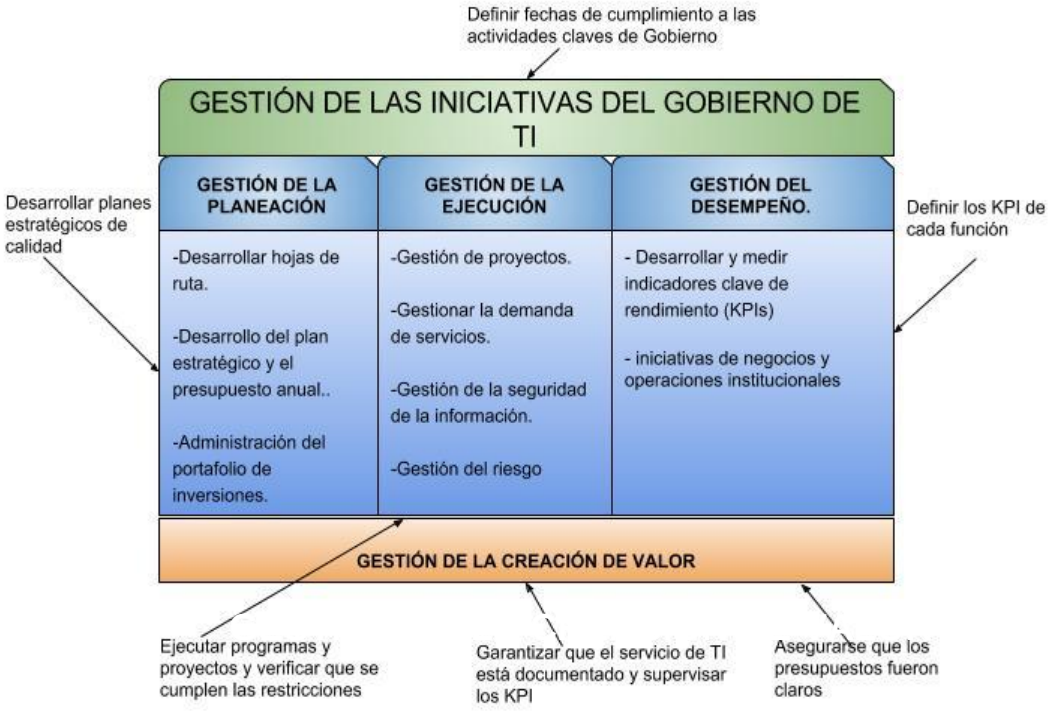


Figura 6: Gestión de iniciativas desde las Áreas clave del gobierno de TI.

Fuente: adaptado de Selig G, Implementing IT Governance, 2010.

4.12 MATRIZ TOMA DE DECISIONES PARA GOBIERNO DE TI EN LA CONTRALORÍA.

A continuación se define claramente las funciones y alcances relacionados con la autoridad y la toma de decisiones mediante la elaboración de la matriz de decisión para la Contraloría territorial de la Guajira. En donde se asignan los responsables para cada rol y se definen los niveles de autoridad para las principales áreas de TI lo que nos permite eliminar confusiones y definir el alcance de la decisión.

Componente de Gobierno de TI	Entrada a la decisión	Autoridad de decisión	Comentarios
Principios de TI (Declaración de alto nivel sobre cómo será utilizado TI para generar valor agregado (ROI) en la Contraloría).	Contralor	- CIO - Director de TI	- Define políticas de TI. - Plan estratégico de TI.
Plan de inversión, factores claves de éxito e indicadores claves de rendimiento.	Contralor	- Contralor - Director de TI	- El presupuesto es revisado por el director de TI y aprobado por el Contralor. - Medición del desempeño (KPI). - BSC.
- Implementación de SGSI en la Contraloría.	Contralor	- Director de TI	- El director de TI diseña y gestiona y el contralor aprueba la financiación e implementación de proyectos de SGSI.
- Infraestructura de TI, Proveedores y terceros.	- Director de TI - Contralor	- Director de TI - Contralor	- Gestiona y aprueba el outsourcing de servicios.

Tabla 3. Matriz de Toma de decisiones para Gobierno de TI
Fuente: adaptado de Selig, G, Implementing IT Governance.

4.13 DIRECCIONES, COMITÉS, FUNCIONES Y GOBERNANZA DE TI EN LA CONTRALORÍA.

Las compañías con mejor desempeño tienen definidos equipos de trabajo multidisciplinares organizados en diferentes niveles jerárquicos y cargos establecidos en los cuales tienen sus funciones y responsabilidades claras para garantizar el cumplimiento de los compromisos adquiridos, comunicaciones más eficaces, retorno de la inversión (ROI) y garantizar la continuidad del negocio.

Es necesario definir cargos de nivel directivo, comités y funciones claras para la implementación de las mejores prácticas (COBIT 5 e ISO 27001) en la Contraloría que permitan alinear la estrategia de gobierno de TI con los objetivos de la entidad y gestionar la seguridad de la información.

¿Por qué son importantes?

Ayudan a asegurar la alineación en todas las partes de una organización; cuando la demanda de recursos para TI supere lo presupuestado, definirá prioridades.

Proporcionan el espacio necesario para la toma de decisiones en materia de inversión.

Construyen una visión empresarial y ayudar a eliminar los sistemas duplicación de esfuerzo en toda la organización.

¿En qué deberían enfocarse?

El contralor y La junta directiva y/o comité de trabajo:

Revisar y aprobar planes estratégicos, programas / proyectos importantes y

Establecer prioridades entre estos y garantizar que todos estén alineados con los objetivos organizacionales.

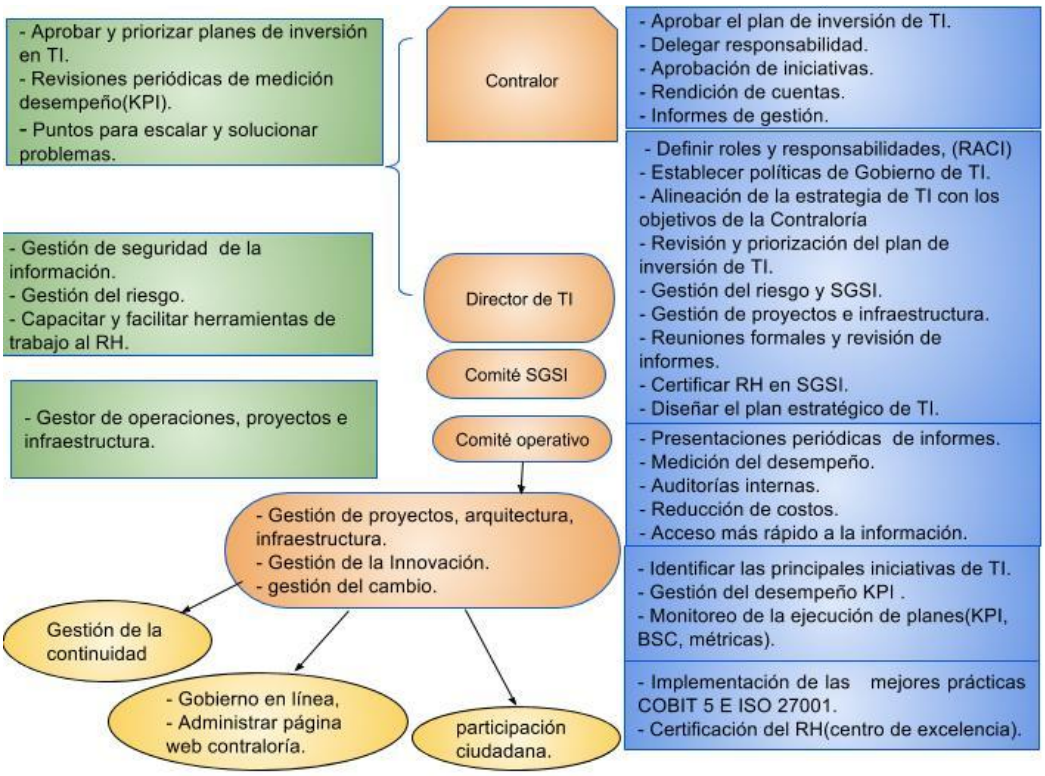


Figura 7: Direcciones, comités y funciones de dirección y gobernanza de TI en la Contraloría.
Fuente: adaptado de Selig, G, Implementing IT Governance.

4.14 MÉTRICAS Y MODELO DE MADUREZ

El Modelo de Madurez de Capacidades o CMM, es un modelo diseñado para evaluar los procesos de una organización, nos permite identificar si la estrategia de TI está alineada con los objetivos de la Contraloría y nos permite identificar el nivel de madurez actual así como las acciones que se deben tomar para llegar a un nivel de madurez deseado, el cual va a estar influenciado por los objetivos de la contraloría y el entorno de la misma. Selig (2010)

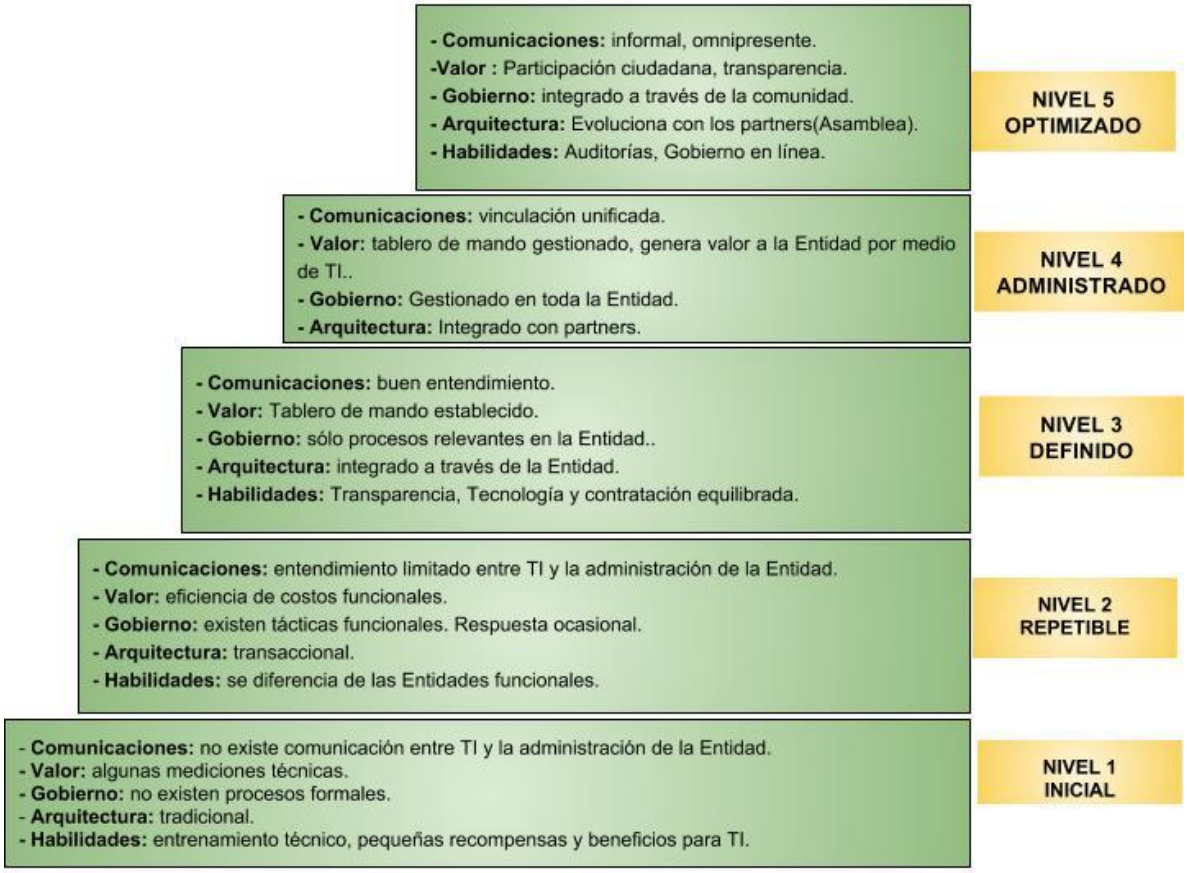


Figura 8: Modelo de Madurez CMM
Fuente: Tomado de Selig, G, Implementing IT Governance

5 MARCOS DE REFERENCIA

5.1 COBIT 5

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público. (ISACA, 2012).

5.1.1 PRINCIPIOS DE COBIT 5.

COBIT 5, se basa en cinco principios claves para el gobierno y la gestión de las TI empresariales, los cuales se muestran en la Figura 6.

Figura 9. Principios de COBIT 5
Fuente: COBIT 5: Un marco de negocio para el Gobierno y la Gestión de la Empresa, (ISACA, 2012)

Principio 1: Satisfacer las Necesidades de las Partes Interesadas.

COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. Permitiendo que las empresas puedan desarrollar su función de crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. Pero, como todas las empresas no tienen los mismos objetivos, cada una puede personalizar COBIT 5 adaptándolo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeado con procesos y prácticas específicos.

Principio 2: Cubrir la Empresa Extremo a Extremo.

COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo, es decir, cubre todas las funciones y procesos dentro de la empresa, no se enfoca sólo en la “función de TI”, sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa. Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos, tanto internos como externos, los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas.

Principio 3: Aplicar un Marco de Referencia único integrado.

Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las Ti de la empresa.

Principio 4: Hacer Posible un Enfoque Holístico.

Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores (enablers) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo COBIT 5 define siete categorías de catalizadores:

- ✓ Principios, Políticas y Marcos de Trabajo.
- ✓ Procesos.
- ✓ Estructuras Organizativas.
- ✓ Cultura, Ética y Comportamiento.
- ✓ Información.
- ✓ Servicios, Infraestructuras y Aplicaciones.
- ✓ Personas, Habilidades y Competencias

Principio 5: Separar el Gobierno de la Gestión.

El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. La visión de COBIT 5 en esta distinción clave entre gobierno y gestión es:

- **Gobierno:**

Asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas

acordadas. En muchas corporaciones, el gobierno global es responsabilidad del comité de dirección bajo el liderazgo del presidente. Algunas responsabilidades de gobierno específicas se pueden delegar en estructuras organizativas especiales al nivel apropiado, particularmente en las corporaciones más grandes y complejas.

- **Gestión**:

Planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales. En muchas empresas, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del Director General Ejecutivo (CEO).

5.1.2 INTERACCIÓN ENTRE GOBIERNO Y GESTIÓN.

De acuerdo con los conceptos anteriores de gobierno y gestión, queda claro que comprenden diferentes tipos de actividades, con diferentes responsabilidades; sin embargo, dado el papel de gobierno: evaluar, orientar y vigilar, se requiere entonces de un conjunto de interacciones entre gobierno y gestión para obtener un sistema de gobierno eficiente y eficaz. Estas interacciones, empleando una estructura de catalizadores, se dan a alto nivel en las organizaciones, como se aprecia en la siguiente tabla.

Catalizador	**Interacciones**
Procesos	En el ilustrativo modelo de procesos de COBIT 5 (COBIT 5: Procesos Catalizadores), se distingue entre los procesos de gobierno y de gestión, incluyendo conjuntos específicos de prácticas y actividades para cada uno. El modelo de procesos también incluye una matriz RACI que describe las responsabilidades de las diferentes estructuras organizativas y roles en la empresa.
Información	El modelo de procesos describe las entradas y salidas de los distintos procesos basados en prácticas a otros procesos, incluyendo la información intercambiada entre los procesos de gobierno y gestión. La información empleada en evaluar, orientar y supervisar la TI empresarial es intercambiada entre gobierno y gestión tal y como se describe en las entradas y salidas del modelo de procesos.
Estructuras Organizativas	En cada empresa, se definen varias estructuras organizativas; en función de su composición y ámbito de decisiones, las estructuras pueden ubicarse en el área

	de gobierno o en el de gestión. Dado que el gobierno trata acerca de establecer la orientación, la interacción tiene lugar entre las decisiones tomadas por las estructuras de gobierno - por ejemplo, decidir sobre la cartera de inversiones y establecer el umbral de riesgo - y las decisiones y operaciones que las implementan.
Principios, Políticas y Marcos	Los principios, políticas y marcos son los vehículos mediante los cuales las decisiones de gobierno son sancionadas en la empresa, y por esa razón son una interacción entre las decisiones de gobierno (establecer orientaciones) y gestión (ejecutar las decisiones).
Cultura, Ética y Comportamientos	El comportamiento también es un catalizador clave del buen gobierno y la gestión empresarial. Se establece al más alto nivel (liderando mediante el ejemplo) y es, por tanto, una interacción importante entre el gobierno y la gestión.
Personas, Habilidades y Competencias	Las actividades de gobierno y de gestión requieren conjuntos de habilidades distintas, pero una habilidad esencial para miembros tanto del órgano de gobierno como de gestión es entender tanto las propias actividades como cuáles son sus diferencias.
Servicios, Infraestructura y Aplicaciones	Se requieren servicios, soportados por las aplicaciones e infraestructura, para proporcionar la información adecuada al órgano de gobierno y soportar las actividades de gobierno a la hora de evaluar, establecer la orientación y supervisar

Tabla 4. Interacciones entre Gobierno y Gestión en COBIT 5.
Fuente: ISACA (2012)

5.1.3 DOMINIOS Y PROCESOS DE COBIT 5.

COBIT 5 incluye un modelo de referencia de procesos que define y describe en detalle varios procesos de gobierno y de gestión. Dicho modelo representa todos los procesos que normalmente encontramos en una empresa relacionados con las actividades de TI, proporciona un modelo de referencia común entendible para las operaciones de TI y los responsables de negocio.

El modelo de referencia de procesos de COBIT 5 divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos:

• **Gobierno**: Contiene cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (EDM)

. • **Gestión**: Contiene cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar (Plan, Build, Run and Monitor - PBRM), y proporciona cobertura extremo a extremo de las TI. Estos dominios son una evolución de la estructura de procesos y dominios de COBIT 4.1. Los nombres de estos dominios han sido elegidos de acuerdo a estas designaciones de áreas principales, pero contienen más verbos para describirlos:

– Alinear, Planificar y Organizar (Align, Plan and Organise, APO)

– Construir, Adquirir e Implementar (Build, Acquire and Implement, BAI)

– Entregar, dar Servicio y Soporte (Deliver, Service and Support, DSS)

– Supervisar, Evaluar y Valorar (Monitor, Evaluate and Assess, MEA)

Cada dominio posee un número de procesos que además de los definidos en COBIT 4.1, integra también los modelos de procesos de Risk IT y Val I. En total se definen 37 procesos, los cuales se observan en la siguiente figura, estos hacen parte del modelo de referencia

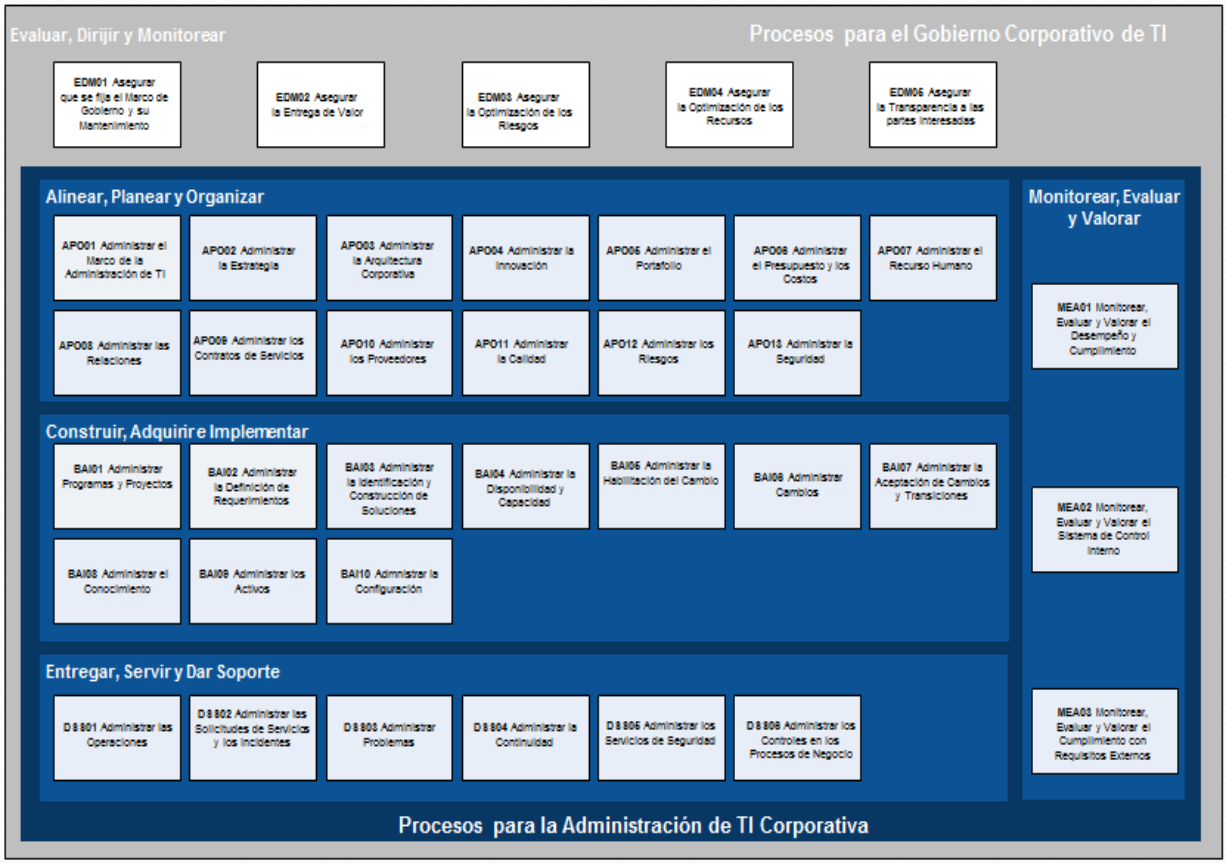


Figura 10: Dominios y procesos de COBIT 5.

Fuente: COBIT 5, ISACA 2012

5.2 NORMA ISO/IEC 27001:2013

Esta Norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de la seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales empleados,

y el tamaño y estructura de la organización. Se espera que todos estos factores de influencia cambien con el tiempo.

El sistema de gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente.

Es importante que el sistema de gestión de la seguridad de la información sea parte de los procesos y de la estructura de gestión total de la información de la organización y que esté integrado con ellos, y que la seguridad de la información se considere en el diseño de procesos, sistemas de información y controles. Se espera que la implementación de un sistema de gestión de seguridad de la información se difunda de acuerdo con las necesidades de la organización.

La presente Norma puede ser usada por partes internas y externas para evaluar la capacidad de la organización para cumplir los requisitos de seguridad de la propia organización.

5.3 NORMA ISO/IEC 27002:2013

ISO / IEC 27002 en su versión 2013 es una guía que proporciona directrices para los estándares de seguridad de la información de la organización y las prácticas de gestión de seguridad de la información, incluida la selección, implementación y gestión de los controles, teniendo en cuenta el medio ambiente riesgo seguridad de la información de la organización, esta norma contempla 14 Dominios, 35 Objetivos de Control y 114 Controles y se encuentra contendía en el anexo de a Norma ISO 27001.

Está diseñado para ser utilizado por las organizaciones que pretenden:

- ✓ Seleccionar los controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información basado en ISO / IEC 27001;

- ✓ Implementar controles de seguridad de la información generalmente aceptadas;
- ✓ Desarrollar sus propias directrices de gestión de seguridad de la información. (ISO, 2013)

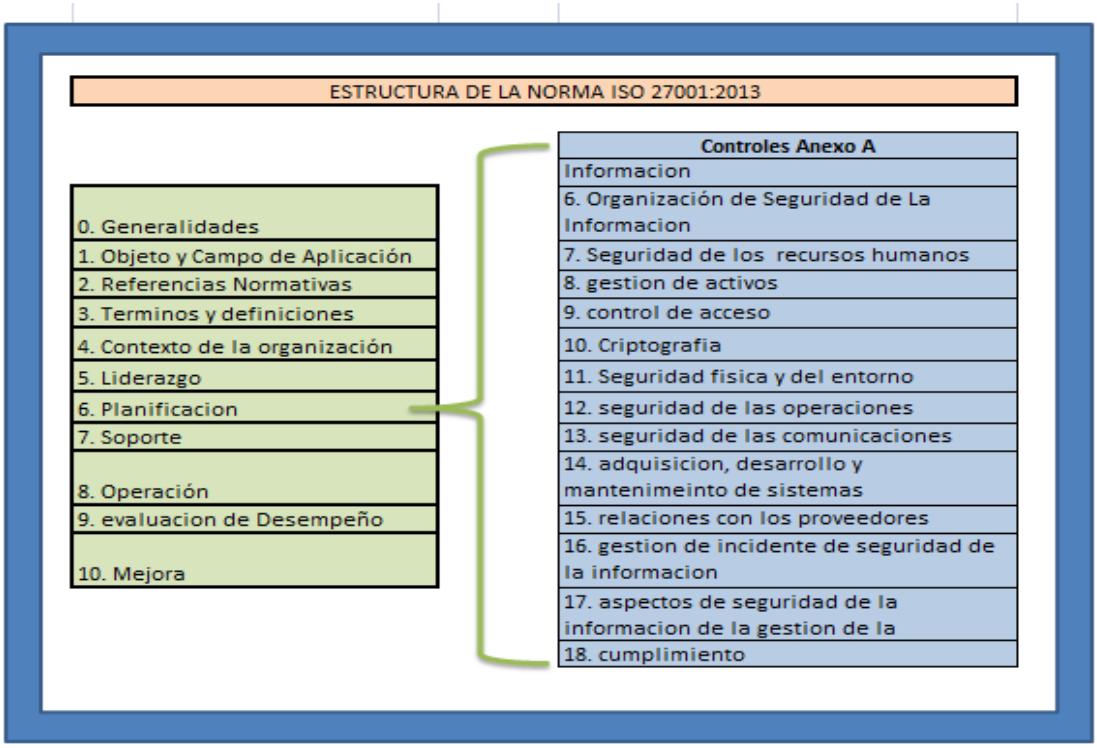


Figura 11: Dominio y objetivos de control de la norma ISO/IEC 27001:2013
Fuente: Elaboración Propia.

5.4 ALINEACIÓN DE LOS PROCESOS DE COBIT 5.0 E ISO 27001:2013 EN TORNO A LA SEGURIDAD DE LA INFORMACIÓN

Johann Tello Meryk, Director de Latam Consulting Services, en su participación en la Conferencia Latinoamericana CACS/ISRM 2014, organizada por ISACA, presentó una ponencia denominada “Mapeando Fortalezas de COBIT 5 Seguridad con ISO/IEC 27001:2013”, de allí se extrae lo siguiente:

COBIT 5 con relación a la Seguridad de la Información tiene los siguientes fines:

Asegurar que dentro de la empresa, la información está protegida contra la divulgación por usuarios no autorizados (confidencialidad), modificación inapropiada (integridad) y no acceso cuando es requerida (disponibilidad).

- ✓ Confidencialidad significa preservar restricciones autorizadas en el acceso y divulgación, incluyendo la protección de privacidad y propietario de la información.
- ✓ Integridad significa guarda contra la modificación inapropiada o destrucción e incluye asegurarse de la no repudiación de la información y su autenticidad.
- ✓ Disponibilidad significa asegurarse del acceso oportuno y fiable a la información y su uso.

Por su parte ISO 27001: 2013 es decir, el sistema de administración de la seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de administración de riesgo y brinda confianza a las partes interesadas que el riesgo está adecuadamente administrado.

Es importante que el sistema de administración de la seguridad de la información es parte y está integrado con los procesos de la organización y con la estructura global de la gerencia y que la seguridad de la información es considerada en el diseño de procesos, sistemas de información y controles. La expectativa es que la implementación del sistema de administración de la seguridad de la información será escalada en concordancia con las necesidades de la organización.

En la siguiente tabla se muestra la relación de los procesos de COBIT 5.0 y los Objetivos de Control y Controles de ISO 27001:2013:

DOMINIO	COBIT 5.0		ISO 27001:2013
Evaluar, Dirigir y Monitorear	EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	5.1 Liderazgo y compromiso 5.2 Política 5.3 Roles, responsabilidades y autoridades organizacionales 6.2 Objetivos de seguridad de la información y la planeación para su logro 7.4 Comunicación A.5 Política de Seguridad de Información
	EDM02	Asegurar la entrega Beneficios	4.1 Entendiendo a la organización y su contexto 4.2 Entender las necesidades y expectativas de las partes interesadas 6.1.1 General 9.3 Revisión Gerencial 10 Mejoramiento
	EDM03	Asegurar la optimización del Riesgo	5.2 Política 6.1 Acciones para abordar los riesgos y las oportunidades 7.5 Información documentada 8.1 Plan operacional y de control 8.3 Tratamiento al riesgo de seguridad de información 9.1 Monitoreo, medición, análisis y evaluación 9.3 Revisión gerencial
	EDM04	Asegurar la optimización de recursos	4.4 Sistema de Administración de la seguridad de información 7.1 Recursos 7.2 Competencia 7.3 Concienciación
	EDM 05	Asegurar la transparencia hacia las partes interesadas	A.12 Operaciones de Seguridad
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de gestión de TI	5 Liderazgo A.5 Política de seguridad de la información A.6 Organización de seguridad de la información
	APO02	Gestionar de Estrategia	4 Contexto de la organización 5.2 Política 6 Planeación
	APO03	Gestionar la Arquitectura Empresarial	
	APO04	Gestionar la innovación	
	APO05	Gestionar el portafolio	
	APO06	Gestionar el Presupuesto y Costos	
	APO07	Gestionar el Recurso Humano	7.2 Competencia 7.3 Concienciación

			A.7 Seguridad de Recursos Humanos
	APO08	Gestionar las relaciones	A.6.1 Organización interna
	APO09	Gestionar acuerdos de servicios	
	APO10	Gestión de Proveedores	A.15 Relación con proveedores
	APO11	Gestiona de la Calidad	4.1 Entendiendo la organización y su contexto 4.2 Entender las necesidades y expectativas de las partes interesadas 6.1.1 General 9.3 Revisión gerencial 10 Mejoramiento
	APO12	Gestión de Riesgo	5.2 Política 6.1 Acciones para abordar los riesgos y las oportunidades 7.5 Información documentada 8.1 Plan operacional y de control 8.3 Tratamiento al riesgo de seguridad de información 9.1 Monitoreo, medición, análisis y evaluación 9.3 Revisión gerencial
	APO13	Gestionar seguridad	Considerado en todo el estándar
Construir, adquirir e implementar	BAI01	Gestión de Programas y Proyectos	
	BAI02	Gestionar la definición de requisitos	A.18 Cumplimiento
	BAI03	Gestionar la identificación y construcción de soluciones	A.14 Adquisición, desarrollo y mantenimiento de sistemas
	BAI 04	Gestionar la disponibilidad y capacidad	A.12.1.3 Administración de capacidad
	BAI 05	Gestionar la introducción del cambio organizativo	
	BAI06	gestionar los cambios	A.12.1.2 Administración de cambios
	BAI 07	Gestionar la aceptación del cambio y la transición	A.12.1.4 Separación de los ambientes de desarrollo, prueba y operaciones
	BAI 08	Gestión del Conocimiento	7.5 Información documentada
	BAI09	Gestión de los activos	A.8 Administración de activos
	BAI10	gestionar configuración	
Entrega, servicio y soporte	DSS01	gestión de operaciones	6.1 Acciones para abordar los riesgos y oportunidades 8 Operaciones A.11 Seguridad física y ambiental

			A.12.3 Respaldos A.12.4 Monitoreo y registro A.15 Relación con proveedores
	DSS02	Gestionar peticiones e incidentes de servicios	A.16 Administración de incidentes de seguridad de la información
	DSS03	Gestionar problemas	
	DSS04	Gestionar la Continuidad	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 7.5 Información documentada 10 Mejoramiento
	DSS05	Gestionar servicios de seguridad	Considerado en todo el estándar
	DSS 06	Gestionar Controles de Procesos de Negocios	6.1.2 Evaluación de riesgo de seguridad de la información 9 Evaluación del rendimiento A.8.2 Clasificación de la información A.9.4 Control de acceso a los sistemas y aplicaciones
Monitorear, evaluar y valorar	MEA01	Supervisar, evaluar y valorar el rendimiento y la conformidad.	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 9 Evaluación del rendimiento
	MEA02	supervisar, evaluar y valorar el sistema de control interno	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 9 Evaluación del rendimiento A.18.2 Revisiones de seguridad de la información
	MEA03	supervisar, evaluar y valorar la conformidad con los requisitos externos	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 9 Evaluación del rendimiento A.18.1 Cumplimiento con requerimientos legales y contractuales

TABLA 5: Mapeo procesos COBIT 5 e ISO 27001:2013
Fuente: Tomado de “Mapeando Fortalezas de COBIT 5 Seguridad con ISO/IEC 27001:2013”,

El autor como conclusión determina lo siguiente:

- COBIT 5 para Seguridad de la Información nos brinda un marco de gobierno de seguridad alineado a ISO 27001:2013.
- Ambos estándares establecen como requerimientos principales para la seguridad de la información:
    - Entendimiento de la organización
    - Las necesidades y expectativas
    - Compromiso de la alta gerencia
    - Roles y responsabilidades
    - Planeación
    - Evaluar y tratar el riesgo
    - Medir resultados
    - Documentar
    - Mejoramiento continuo
- Comparten las mismas preocupaciones sobre la integridad, confidencialidad e integridad de la información.
- Las inversiones en seguridad de la información sólo serán sostenibles a través del cumplimiento de estándares.

5.5 NORMA ISO 31000: GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES

Esta norma brinda los principios y las directrices genéricas sobre la gestión del riesgo, puede ser utilizada por cualquier empresa pública, privada o comunitaria, asociación, grupo o individuo. Por lo tanto, no es específica para ninguna industria o sector.

Esta norma se puede aplicar durante toda la duración de una organización y a un amplio rango de actividades, incluyendo estrategias y decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos.

Esta norma se puede aplicar a cualquier tipo de riesgo, cualquiera sea su naturaleza, bien sea que tenga consecuencias positivas o negativas.

El éxito de la gestión del riesgo dependerá de la eficacia del marco de referencia para la gestión, el cual brinda las bases y las disposiciones que se introducirán en todos los niveles de la organización. El marco ayuda a la gestión eficaz del riesgo a través de la aplicación del proceso para la gestión del riesgo (véase el numeral 5) en los diversos niveles y en contextos específicos de la organización. El marco garantiza que la información acerca del riesgo derivada del proceso para la gestión del riesgo se reporte de manera adecuada y se utilice como base para la toma de decisiones y la rendición de cuentas en todos los niveles pertinentes de la organización.

Este numeral describe los componentes necesarios del marco para gestionar el riesgo y la forma en que ellos se interrelacionan de manera reiterativa, tal como se ilustra en la siguiente Figura.

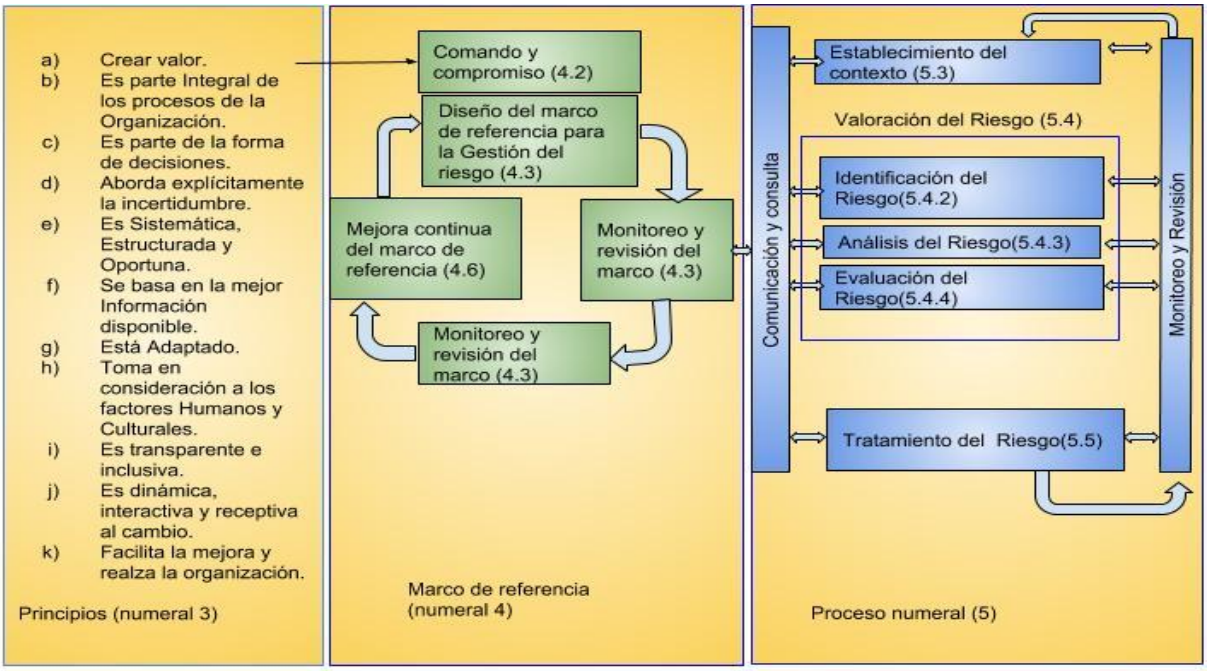


Figura 12: Elementos de la Norma ISO 31000
Fuente: adaptado de la Norma NTC/ ISO 31000

6 MARCO REFERENCIAL

De acuerdo con Schwarz (2013), se entiende como estado del arte a la base más profunda de la investigación que permite descubrir un conocimiento nuevo al revisar la literatura asociada al tema de investigación que permite determinar quiénes, cómo, cuándo, dónde y por qué han tratado de resolver el problema de investigación, determinar su actualización y verificar si el tema sigue vigente así como descubrir hasta dónde ha avanzado el conocimiento validado más reciente sobre el tema en el que se está trabajando, además cuales son los aportes para desarrollar una nueva investigación

A partir de la anterior concepción, se relacionan las tesis tomadas como referencia para desarrollar la presente investigación, estos proyectos en cuanto a su contenido, son próximos a lo que se pretende realizar.

Los modelos estudiados presentan elementos, conceptos y enfoques que pueden ser considerados, reusados y adaptados a los requisitos del modelo a construir los cuales se relacionan a continuación.

La tabla presentada a continuación contiene el resumen de los artículos utilizados como material de apoyo en esta investigación. La fuente de estos artículos fue IEEE.org y consultados durante los meses de junio a noviembre de 2016.

Tabla de resumen de las tesis de maestría utilizadas como referencia para el desarrollo de esta investigación.

TÍTULO	FRAMEWORK PARA GOBIERNO ESTRATÉGICO DE TI BASADO EN COBIT, ITIL E ISO 27000 GOITA: Gobierno Alineado de TI (Government IT Alignment)
UNIVERSIDAD- TIPO DE PUBLICACIÓN – AÑO	Universidad del Norte - Tesis de Maestría - 2011

AUTORES:	MARÍA GISELA LÓPEZ CASTILLO BELKYS POSSO ESCORCIA Dirigido por: Ph.D. Wilson Nieto
OBJETIVO	Formular y diseñar un marco estratégico de gobierno de TI para una organización con características similares a la descrita anteriormente, a partir de la alineación de los marcos de trabajo de COBIT, ITIL e ISO 27000.
RESUMEN	En el desarrollo del trabajo referenciado, se observa la alineación del marco de trabajo COBIT 4.1 con la norma ISO 27002 e ITIL V3, lo que produce un marco de referencia único denominado GOITA, el cual apoya el trabajo que vamos a realizar en la entidad Contraloría General del Departamento de La Guajira, actualizando a las versiones de COBIT 5 e ISO 27002 en su versión 2013.
CONCLUSIÓN	Luego de lo expuesto se puede mencionar como conclusión final que existe una problemática en cuanto a cómo se debe manejar la gestión de las Tecnologías en las empresas; Los diferentes marcos de trabajo aportan valiosas guías que pretenden solucionar dichos problemas. Sin embargo, se debe tener claro cuáles estándares son más útiles de acuerdo con las necesidades de las compañías de qué manera se pueden integrar los que se usen. Estos estándares son la base para lograr un buen Gobierno de TI, A su vez, este buen gobierno permitirá alcanzar las metas planteadas en relación con las inversiones en TI, la gestión de los riesgos, recursos y alineamiento estratégico.

TÍTULO	DISEÑO DE UNA METODOLOGÍA PARA LA IMPLEMENTACIÓN DE UN MARCO DE GOBIERNO DE TI EN LAS PYMES COLOMBIANAS DEL BASADO EN COBIT 4.1
UNIVERSIDAD-TIPO DE PUBLICACIÓN – AÑO:	Universidad del norte -Tesis de Maestría - 2011
AUTORES:	MONICA SOTO CAMARGO GUSTAVO MORALES CARPIO Dirigido por: Ph.D. Wilson Nieto
OBJETIVO	Diseñar una metodología para la implementación de un marco de gobierno de TI en las Pymes colombianas basado en COBIT 4.1.
RESUMEN	El documento referenciado, presenta una metodología adecuada para la implementación del Gobierno de TI, basado en el estándar COBIT 4.1, con pautas que nos pueden ayudar para definir la propuesta de implementación

	del Modelo propio para la Contraloría General del Departamento de La Guajira, integrando en esta oportunidad la versión 5 de COBIT y la norma ISO del año 2013.
CONCLUSIÓN	Simplificar la implementación de un Gobierno de TI a través de una metodología para las pymes puede ayudarles a incorporar las TI, organizar los procesos y recursos existentes, compararse con otras organizaciones de una manera simple e inclusive visualizar nuevas oportunidades de negocio.

TÍTULO	Protocolo para Gestionar Procesos B2C en el Contexto de Organizaciones Académicas.
UNIVERSIDAD-TIPO DE PUBLICACIÓN – AÑO:	Universidad del norte -Tesis de Maestría
AUTORES:	Pierre Julliard Amador.
OBJETIVO	Diseñar un protocolo organizacional para la Gestión B2C en instituciones Universitarias.
CONCLUSIÓN	Luego de estudiar detalladamente una gran variedad de marcos de gestión de TI hemos encontrado que tienen grandes similitudes, porque todos buscan que se mejoren los Métodos, se determinen responsabilidades y se creen estructuras de gobierno.

TÍTULO	Marco de gobierno general para la administración efectiva de los activos y estrategias de Tecnología Informática (TI) en la Universidad del Norte, que integre los procesos y dominios desde los estándares COBIT™, ITIL™ y Val IT™.
TIPO DE PUBLICACIÓN - AÑO:	Universidad del Norte - Tesis de Maestría - 2011
AUTORES:	LILIANA ARTETA MOLINA JOHN FLÓREZ TORRES Dirigido por: Ph.D. Wilson Nieto
OBJETIVOS	Diseñar y estructurar un marco de gobierno general para la administración efectiva de los activos y estrategias de Tecnología Informática (TI) en la Universidad del Norte, que integre los procesos y dominios desde los estándares COBIT™, ITIL™ y Val IT™.
RESUMEN	Análisis y evaluación del estado del arte de gobierno de TI; para esto se

	analizaron a profundidad los estándares COBIT™ 4.1 y Val IT™ 2.0 y las mejores prácticas de ITIL™ Realización de un diagnóstico organizacional de gobierno de TI en la Universidad a partir de los procesos de alto nivel de COBIT™, Val IT™ e ITIL™. Con este diagnóstico se estableció el nivel de madurez actual de cada uno de los procesos de TI.
CONCLUSIÓN	Es recomendable usar todos ellos en conjunto al mismo tiempo dado que esto crea retos de integración por resolver. Se pueden adaptar piezas de cada uno de manera personalizada en la organización y aplicarlas de acuerdo al énfasis para el cual fue desarrollado. Este lineamiento fue aplicado en este trabajo de grado.

TÍTULO	Gobierno Estratégico de TI caso aplicado para las empresas del sector de las telecomunicaciones
TIPO DE PUBLICACIÓN - AÑO:	Universidad del Norte - Tesis de Maestría - 2010
AUTORES:	CASALINS GRANADOS, ZAMIR Dirigido por: Ph.D. Wilson Nieto
OBJETIVOS	Formular y diseñar un marco de gobierno estratégico de TI como referente para las empresas del sector de las telecomunicaciones, soportado en las mejores prácticas y estándares mundialmente aceptados en Gobierno de TI.
RESUMEN	Se interpretó los marcos de referencia, documentos, artículos y casos de estudio que generan el conocimiento suficiente relacionado con Gobierno de TI y su gestión, planeación estratégica, modelos de procesos de negocio, medición de desempeño y arquitectura empresarial. Seguidamente se diagnosticó de procesos de gobierno de TI a partir de control de procesos de alto nivel, entrevistas. Lo que permitió la revisión la cultura organizacional con respecto a procesos de gobierno de TI. Posteriormente se definieron las políticas y procesos que abarcan los 4 dominios de gobierno de TI con los roles y responsables de su ejecución y cumplimiento buscando darle forma al marco de gobierno para ejecutivos. En consecuencia se definió y ejecutó el despliegue de las diferentes políticas y procesos como parte del marco de gobierno de TI integrándose con los procesos y cultura organizacional. Finalmente se realizó nuevamente un diagnóstico de las políticas y procesos del marco de gobierno de TI y la identificación de brechas y acorde con esto ejecutar procesos de mejora continua.
CONCLUSIÓN	El procedimiento de mejoramiento continuo estratégico planteado y el uso del Balanced Scorecard como herramienta de apoyo para la medición del avance o logro de los objetivos estratégicos de TI, permiten facilitar la comunicación y la gestión que un Gobierno de TI realiza durante la ejecución de la metodología de direccionamiento estratégico planteada. Conocer y entender el mapa de procesos asociados a una empresa específica,

	permite realizar el análisis suficiente para integrar, articular y relacionar los procesos de marcos de referencia ampliamente aceptados para la implementación de un Gobierno de TI y los enfoques propios de este (Alineación estratégica, entrega de valor, administración de riesgo, administración de recursos y medición y desempeño). Con esta integración y relación es como se logra definir aquellas políticas y procesos que apoyan la divulgación y concientización de un Gobierno Estratégico de TI.

TÍTULO	Marco de gobierno general para la administración efectiva de los activos y estrategias de Tecnología Informática (TI) en la Universidad del Norte, que integre los procesos y dominios desde los estándares COBIT™, ITIL™ y Val IT™.
TIPO DE PUBLICACIÓN - AÑO:	Universidad del Norte - Tesis de Maestría - 2011
AUTORES:	LILIANA ARTETA MOLINA JOHN FLÓREZ TORRES Dirigido por: Ph.D. Wilson Nieto
OBJETIVOS	Diseñar y estructurar un marco de gobierno general para la administración efectiva de los activos y estrategias de Tecnología Informática (TI) en la Universidad del Norte, que integre los procesos y dominios desde los estándares COBIT™, ITIL™ y Val IT™.
RESUMEN	Análisis y evaluación del estado del arte de gobierno de TI; para esto se analizaron a profundidad los estándares COBIT™ 4.1 y Val IT™ 2.0 y las mejores prácticas de ITIL™ Realización de un diagnóstico organizacional de gobierno de TI en la Universidad a partir de los procesos de alto nivel de COBIT™, Val IT™ e ITIL™. Con este diagnóstico se estableció el nivel de madurez actual de cada uno de los procesos de TI.
CONCLUSIÓN	Es recomendable usar todos ellos en conjunto al mismo tiempo dado que esto crea retos de integración por resolver. Se pueden adaptar piezas de cada uno de manera personalizada en la organización y aplicarlas de acuerdo al énfasis para el cual fue desarrollado. Este lineamiento fue aplicado en este trabajo de grado.

TÍTULO	Propuesta para la implementación de un esquema de gobierno de Tecnologías de la Información (TI) en ambientes tercerizados (outsourcing). Caso de estudio: Universidad Nacional de Colombia.

TIPO DE PUBLICACIÓN - AÑO:	Universidad Nacional de Colombia, Facultad de Ingeniería, Departamento de Ingeniería de Sistemas e Industrial Tesis de Maestría, 2013
AUTORES:	Adriana Montaña Barón Dirigido por: Ph.D., José Ismael Peña Reyes.
OBJETIVOS	Proponer estrategias para la implementación de un esquema de gobierno de outsourcing de TI en la Universidad Nacional de Colombia.
RESUMEN	La implementación de esquemas de gobierno a nivel de las Tecnologías de la Información es fundamental, contribuye a garantizar el éxito respecto a la prestación de los servicios por medio de la generación de valor y la reducción de los riesgos. La alta dirección, quien actúa como facilitador de gobierno de la organización, debe adoptar estrategias para garantizar el direccionamiento y el monitoreo permanente tanto de la oferta como de la demanda de TI. También debe determinar los modelos de tercerización a utilizar según los tipos de servicio y aplicar prácticas que les permita alinear la estrategia de la organización con los objetivos estratégicos del área de TI. Con base a la consideración anterior y los resultados obtenidos para el diseño del plan estratégico de TI en la Universidad Nacional de Colombia así como la recolección de información respecto al estado actual del sistema de gobierno de los terceros a nivel de TI, se proponen una serie de estrategias que le permitirán a la entidad gobernar la prestación de estos servicios. A largo plazo, lo anterior se convertirá en una ventaja competitiva con la que la Universidad podrá enfrentar activamente los cambios y retos del entorno.
CONCLUSIÓN	En relación con el esquema de gobierno de TI para los servicios que son prestados por terceros, se plantea que el esquema esté basado en tres dimensiones: a. La estructura de gobierno de TI, con la cual se garantiza la coherencia y la eficacia en la gestión de los procesos relacionados con la tercerización de los servicios. b. Los procesos de gobierno de TI comunes (en los que interviene tanto el proveedor como el cliente de servicios). c. El sistema de medición, seguimiento y de gestión de las relaciones y la comunicación con los proveedores.

TÍTULO	Modelo y guía para la implementación de Gobierno de TI en Entidades Bancarias de Colombia
TIPO DE PUBLICACIÓN - AÑO:	Universidad ICESI, Tesis de Maestría, 2010
AUTORES:	María Helena Correa Correa Breyner Alexander Parra Rojas Dirigido por: Ing. Hernando Peña Villamil, MSC.,

OBJETIVOS	Proponer un modelo de Gobierno de TI y una guía para su implementación en entidades bancarias de Colombia, que satisfaga las necesidades legales y corporativas de este sector, teniendo en cuenta que no sería útil aplicar al pie de la letra modelos de Gobierno de otros sectores colombianos, ya que la infraestructura, tecnología, modelo de negocio y sobre todo, legislación, es diferente. Tampoco es pertinente aplicar exactamente modelos de gobierno de TI bancario de otros países dadas las diferencias culturales, operativas, económicas y de legislación existentes con respecto a Colombia.
RESUMEN	Los Bancos dependen hoy en día de TI para su funcionamiento y desarrollo, y hacen grandes esfuerzos e inversiones en tecnología con el objetivo de ser más eficientes y más seguros, sin embargo, el problema es que hasta ahora, no existía un modelo de Gobierno de TI adaptado a las necesidades del sector bancario colombiano.
CONCLUSIÓN	Para la realización de este trabajo se partió de una ventaja significativa y es el hecho que el sector bancario colombiano esta agrupado y regulado por leyes, impartidas mayoritariamente por la superintendencia financiera, las cuales hacen que este sector tenga una estructura organizacional y documental muy bien establecida, lo que allana el camino para una posible implementación de Gobierno de TI. Entre estas leyes está la circular 014 de 2009, la cual obliga al sector bancario a contar con 19 requerimientos de TI, los cuales deben estar documentados y alineados con los objetivos estratégicos de la organización.

7 FRAMEWORK METODOLÓGICO PROPUESTO

Con el fin de poder definir un modelo estándar de gobierno y gestión estratégica de TI, que sirva como referencia para las entidades de control de nivel territorial (en este caso las Contralorías Municipales, Distritales o Departamentales), es necesario iniciar con proponer un modelo de Gobierno y gestión Corporativo, que reúna las características principales de estas organizaciones, teniendo en cuenta las funciones legales que deben cumplir, para lo cual se define una estructura organizativa Genérica, tomando como referencia lo dispuesto en la norma NTC ISO 38500.

7.1 GOBIERNO CORPORATIVO

Esta sección comprende el nivel gerencial de la organización e interrelaciona a todas las partes interesadas de las empresas (internas o externas), de la cual hacen parte los siguientes:

Partes Interesadas Externas:

- ✓ Ciudadanía
- ✓ Proveedores
- ✓ Estado colombiano (reguladores)
- ✓ Entidades departamentales y/o municipales que son sujetos de control de la Contraloría.

Partes Interesadas Internas

- ✓ Empleados

Dentro de la estructura de G&G Corporativo, se encuentran los siguientes entes:

Contralor Territorial: Desde el cual se trazan los lineamientos, políticas y objetivos corporativos, además se encarga de dictar normas generales para armonizar los sistemas de control fiscal de todas las entidades públicas del orden territorial[1].

Auditoría Externa: Como parte de la vigilancia que se realiza sobre las contralorías territoriales, la misma está a cargo de la Auditoría General del República[2],

De igual forma se definen el nivel estratégico, como apoyo, una vez se definen los lineamientos y políticas en el gobierno corporativo, por parte del Contralor Territorial, en la parte estratégica entran a jugar los siguientes:

Comité de Coordinación de Control Interno: El cual se encarga de estudiar y revisar la evaluación del cumplimiento de las metas y objetivos del organismo o entidad, dentro de los planes y políticas sectoriales y recomendar los correctivos necesarios[3].

Comité Directivo: Del cual hacen parte los directivos de las distintas dependencias, quienes se encargan de definir las estrategias necesarias para conseguir los objetivos organizacionales.

Planeación: Se encarga de determinar los planes y programas necesarios para la ejecución de las estrategias planteadas, en coordinación con el comité directivo, además de apoyar el establecimiento de las metas e indicadores necesarios para la medición de estos planes (Acción, Operativo, TI, etc.).

Asesoría Jurídica: Se revisan el cumplimiento de la normatividad vigente aplicable a las Contralorías territoriales, tanto Internas como Externas.

---

[1] Constitución Política de Colombia, Articulo 268.
[2] La Auditoría General de la República es un organismo de vigilancia de la gestión fiscal, dotado de autonomía jurídica, administrativa, contractual y presupuestal el cual está a cargo del Auditor de que trata el artículo 274 de la Constitución Política. Corresponde a la Auditoría General de la República ejercer la vigilancia de la gestión fiscal de la Contraloría General de República, de las contralorías departamentales, distritales y municipales. Sus funciones están definidas en el artículo 17 del Decreto Ley 272 de 2000.
[3] Decreto 1826 del 03 de agosto de 1994, Articulo 2º.

7.2 GESTIÓN CORPORATIVA

En la estructura organizativa genérica, la parte operacional, es la que se encarga de ejecutar las actividades necesarias para el cumplimiento de las metas corporativas, está conformado por los procesos, misionales y de apoyo:

PROCESOS MISIONALES

- Participación ciudadana
- Control fiscal
- Responsabilidad fiscal

PROCESOS DE APOYO

- Talento humano
- Presupuesto y tesorería
- Contabilidad
- Gestión documental - archivo
- Gestión administrativa
- Cobro coactivo
- Tecnología informática

Lo anterior se define en la siguiente figura:

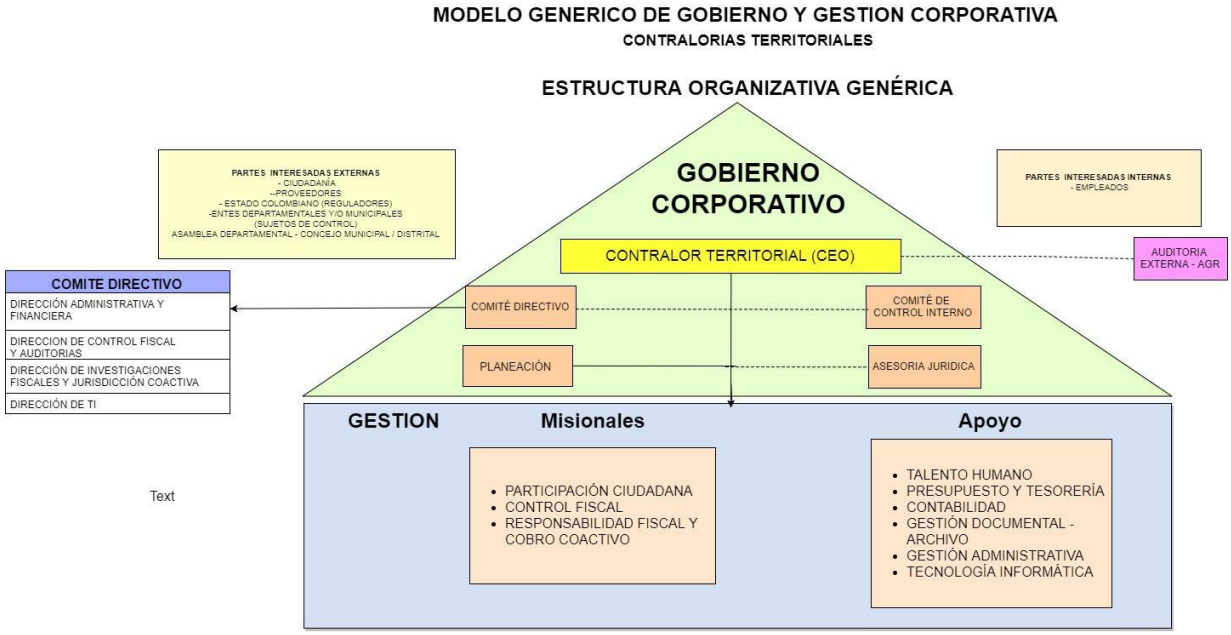


Figura 13: Modelo de G&G Corporativo propuesto para las Contralorías Territoriales
Fuente: Elaboración Propia

7.3 GOBIERNO Y GESTIÓN DE TI

Con el fin de poder definir el modelo de Gobierno y gestión de TI, acorde con el modelo de G&G Corporativo planteado anteriormente, se determinó una estructura organizacional aplicable al área de TI en las entidades de control territorial, en la cual se destaca la gestión de la Seguridad, la gestión de Riesgos, y la Infraestructura que soporta TI, como procesos principales, encaminados a la mejora de la gestión Institucional, como se ve en la siguiente figura:

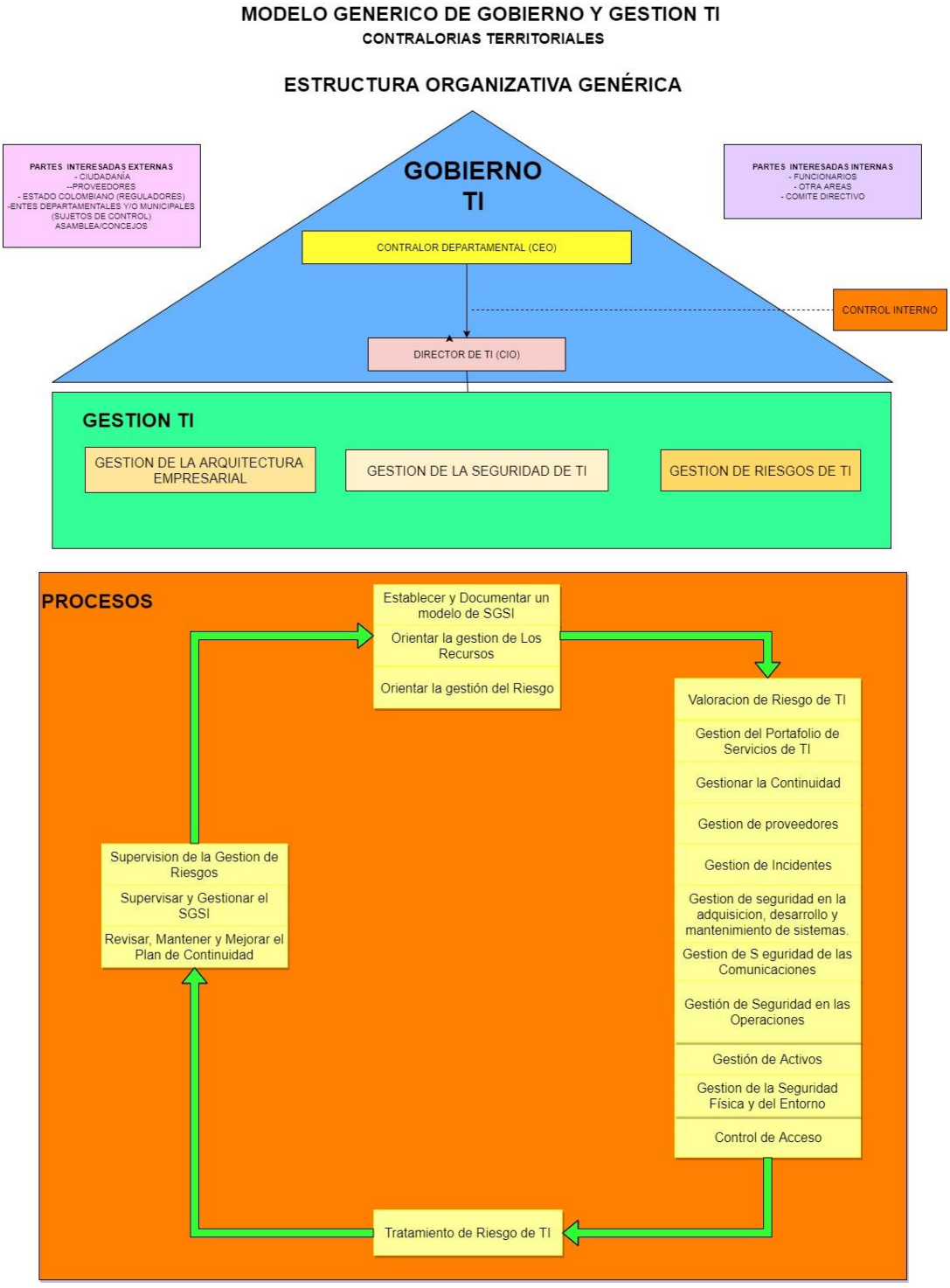


Figura 14: Modelo de G&G de TI propuesto para las Contralorías territoriales
Fuente: Elaboración Propia

7.3.1 OBJETIVOS CORPORATIVOS Y DE TI

Los objetivos Institucionales que sirven como base para este modelo, se definen en términos del BSC, en las diferentes perspectivas, Financiera, Cliente, Interna, Aprendizaje y Crecimiento, sobre ellos se determinan los objetivos de TI que se alinean con la estrategia organizacional, basándonos en los definidos por el marco de referencia COBIT y las funciones institucionales.

PERSPECTIVA BSC	OBJETIVOS CORPORATIVOS	OBJETIVOS DE TI
FINANCIERA	1. Valor para las partes interesadas de las Inversiones de Negocio	Alineamiento de TI y la estrategia de negocio
	2. Riesgos de negocio gestionados (salvaguarda de activos)	Riesgos de negocio relacionados con las TI gestionados
	3. Cumplimiento de leyes y regulaciones externas	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
	4. Transparencia financiera	Optimización de activos, recursos y capacidades de las TI
CLIENTE	5. Cultura de servicio orientada al cliente	Facilidad en la prestación de servicios al ciudadano, utilizando las TI
	6. Continuidad y disponibilidad del servicio de negocio	Seguridad de la información, infraestructuras de procesamiento y aplicaciones
	7. Toma estratégica de Decisiones basada en Información	Disponibilidad de información útil y relevante para la toma de decisiones
INTERNA	8. Optimización de la funcionalidad de los procesos de negocio	Soporte de procesos de la contraloría integrando aplicaciones y tecnología
	9. Programas gestionados de cambio en el negocio	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI
	10. Cumplimiento con las políticas internas	Cumplimiento de TI con las políticas internas de la entidad
APRENDIZAJE Y CRECIMIENTO	11. Personas preparadas y motivadas	Funcionarios capacitados, competentes y motivados
	12. Cultura de innovación de producto y negocio	Conocimiento, experiencia e iniciativas para la innovación en el control fiscal

Tabla 6: Objetivos Corporativos y Objetivos de TI
Fuente: Elaboración Propia

7.3.2 DOMINIOS

CÓDIGO	DOMINIO
PDE	PLANEACIÓN Y DIRECCIÓN ESTRATÉGICA
RTI	GESTIÓN DE RIESGOS
GSI	GESTIÓN DE LA SEGURIDAD
IAS	GESTIÓN DE LA ARQUITECTURA EMPRESARIAL, ADQUISICIÓN Y SOPORTE
TAD	GESTIÓN DEL TALENTO HUMANO, APRENDIZAJE Y DESARROLLO
CEM	CONTROL, EVALUACIÓN Y MEJORA

7.3.3 DETALLE DE PROCESOS DE TI

A continuación se desarrollan cada uno de los dominios, con sus procesos y actividades asociadas.

7.3.3.1 PLANEACIÓN Y DIRECCIÓN ESTRATÉGICA DE TI

Objetivo: Establecer el marco de gobierno de TI que estructure y direccione el flujo de las decisiones de TI que garantice la integración y la alineación con la normatividad vigente, las políticas, los procesos y los servicios de la institución.

Id	Proceso	Id Actividad	Actividad
PDE01	Alineación del Gobierno de TI	PDE01.A01	Documentar la situación actual de la institución, en el contexto organizacional y del entorno, e identificar los factores internos y externos (obligaciones legales, reglamentarias y contractuales) y tendencias que pueden influir en el diseño de gobierno de TI.

PDE02	Esquema de Gobierno de TI	PDE02.A01	Definir las políticas, lineamientos y directrices que hacen parte de la estrategia de Gobierno de TI, de acuerdo con las políticas institucionales de la entidad.
		PDE02.A02	Estructurar e implementar un macro-proceso de gestión de TI que permita direccionar, evaluar y monitorear las capacidades de TI , asegurando el adecuado aprovisionamiento del talento humano y los recursos necesarios para ofrecer los servicios de TI de la institución
		PDE02.A03	Definir los roles y funciones en la estructura de TI, que tienen responsabilidades en la toma de decisiones de TI.
PDE03	Planeación Estratégica de TI	PDE03.A01	Definir el plan estratégico de TI, que incluya la identificación de retos y oportunidades de TI, la definición de políticas e iniciativas estratégicas de TI y la definición del portafolio de proyectos
		PDE03.A03	Definir un tablero de control para medir el avance, el grado de satisfacción de los usuarios frente a los servicios, el desempeño de los procesos y las capacidades, así como los recursos asociados a la estrategia de TI.
PDE04	Informes a las Partes Interesadas	PDE04.A01	Examinar y hacer un juicio sobre los requisitos de notificación obligatoria actuales y futuros relacionados con el uso de las TI dentro de la empresa (regulación, legislación, derecho común, contractual), incluyendo la extensión y frecuencia.
		PDE04.A02	Examinar y hacer un juicio sobre las necesidades actuales y futuras de información para otros grupos de interés relacionados con el uso de las TI dentro de la empresa, incluyendo la extensión y condiciones.
		PDE04.A03	Mantener los principios para la comunicación con los grupos de interés externos e internos, incluyendo los formatos de comunicación y canales de comunicación, y para la aceptación de los interesados y cierre de sesión de presentación de informes.
PDE05	Supervisar la comunicación con las partes interesadas.	PDE04.A04	Evaluar periódicamente la eficacia de los mecanismos para asegurar la exactitud y fiabilidad de la información obligatoria.
		PDE04.A05	Evaluar periódicamente la eficacia de los mecanismos y las salidas de la comunicación con interesados externos e internos.
		PDE04.A06	Determinar si se cumplen los requisitos de los diferentes grupos de interés.
PDE06	Evaluación y Mejora Continua del sistema de gobierno	PDE01.A01	Evaluar periódicamente si los mecanismos para el gobierno de TI acordados (estructuras, principios, procesos, etc.) están establecidos y operando efectivamente.

	de TI.	PDE01.A02	Determinar las acciones que permitan corregir, mejorar y controlar procesos de TI que se encuentren dentro de la lista de no conformidades generada en el marco de las auditorias de control interno y externo, a fin de contribuir con el compromiso de mejoramiento continuo de la administración pública de la institución.

7.3.3.2 GESTIÓN DE RIESGOS DE TI - RTI

Objetivo: Garantizar la optimización del Riesgo, definir los estándares de aceptación y mitigar los efectos en caso de su materialización

Id	Proceso	Id Actividad	Actividad
RTI01	Orientar la gestión de Riesgos	RTI01.A01	Evaluar y entender el contexto, tanto externo como interno de la organización, que influya en el marco de gestión de riesgos de TI.
		RTI01.A02	Definir los criterios que se van a utilizar para evaluar la importancia del riesgo de TI,
		RTI01.A03	Establecer la política para la gestión del riesgo de acuerdo a los objetivos de la organización y el compromiso con ella, acorde con las políticas institucionales.
		RTI01.A04	Identificación de los roles y responsabilidades para la gestión del riesgo de TI
		RTI01.A05	Asignar los recursos adecuados para la gestión del riesgo.
		RTI01.A06	establecer mecanismos para la comunicación interna y la presentación de informes con el fin de ayudar y fomentar la rendición de cuentas y la pertenencia del riesgo
RTI02	Valoración del Riesgo de TI	RTI02.A01	Identificar las fuentes de riesgo de TI, las áreas de impacto, los eventos (incluyendo los cambios en las circunstancias) y sus causas y consecuencias potenciales.
		RTI02.A02	Construir y actualizar regularmente escenarios de riesgo de TI, que incluyan escenarios compuestos en cascada y/o tipos de amenaza coincidentes y desarrollar expectativas para actividades de control específicas, capacidades para detectar y otras medidas de respuesta

		RTI02.A03	Analizar el coste-beneficio de las opciones de respuesta al riesgo potencial, tales como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/capturar. Proponer la respuesta al riesgo óptima.
RTI03	Tratamiento del Riesgo de TI	RTI03.A01	Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. Asegurar que el plan identifica las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los riegos identificados de seguridad de información.
		RTI03.A02	Determinar los controles necesarios para la implementación del Plan de Tratamiento de Riesgos de la Seguridad de la Información, según su aplicabilidad, de acuerdo a los contemplados en el anexo de la norma NTC ISO 27001:2013
		RTI03.A03	Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.
		RTI03.A04	Examinar eventos adversos/pérdidas del pasado y oportunidades perdidas y determinar sus causas raíz. Comunicar la causa raíz, requerimientos de respuesta adicionales para el riesgo y mejoras de proceso a los responsables de toma de decisiones apropiados y asegurarse de que la causa, los requerimientos de respuesta y la mejora del proceso se incluyan en los procesos de gobierno del riesgo.
RTI04	Supervisión de la Gestión de Riesgos	RTI04.A01	Supervisar las metas y métricas clave de gestión de los procesos de gobierno y gestión del riesgo de TI respecto a los objetivos, analizar las causas de las desviaciones e iniciar medidas correctivas para abordar las causas subyacentes.
		RTI04.A02	Revisar la eficacia del marco de referencia para la gestión del riesgo
		RTI04.A03	Tomar decisiones sobre la forma en que se podría mejorar el marco de referencia, la política y el plan para la gestión de los riesgos de TI.

7.3.3.3 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo: Proteger la información de la empresa, a través de la implementación de buenas prácticas de gestión de la seguridad de la información, contemplando todos los factores internos, externos, los riesgos y el cumplimiento de las leyes aplicables.

Identificación proceso	PROCESO	Id Actividad	Actividad
GSI01	Establecer y Documentar el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI)	GSI01.A01	Determinar las cuestiones Internas y externas que son pertinentes para los propósitos de la entidad y que afectan su capacidad para lograr los resultados del sistema.
		GSI01.A02	Determinar las necesidades y expectativas de la Partes Interesadas
		GSI01.A03	Determinar el Alcance del SGSI
		GSI01.A04	Alinear el SGSI con el enfoque global de la gestión de la seguridad en la empresa.
		GSI01.A05	Obtener autorización de la dirección para implementar y operar o cambiar el SGSI.
		GSI01.A06	Definir y documentar la Política de seguridad de la Información que sea adecuada al propósito de la organización, incluya objetivos de seguridad y el compromiso de la dirección para mantener y mejorar el SGSI.
		GSI01.A07	Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.
		GSI01.A08	Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. Asegurar que el plan identifica las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los riegos identificados de seguridad de información.
GSI02	Supervisar y revisar el SGSI.	GSI02.A01	Realizar revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI. Considerar los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas.
		GSI02.A02	Realizar auditorías internas al SGSI a intervalos planificados.
		GSI02.A03	Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.
		GSI02.A04	Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.

		GSI02.A05	Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.
GSI03	Seguridad de los Recursos Humanos	GSI03.A01	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
		GSI03.A02	Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
		GSI03.A03	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
		GSI03.A04	Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
		GSI03.A05	Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
		GSI03.A06	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.
GSI04	Gestión de Activos	GSI04.A01	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
		GSI04.A02	Los activos mantenidos en el inventario deben tener un propietario.
		GSI04.A03	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
		GSI04.A04	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
		GSI04.A05	Se debe desarrollar e implementar procedimientos un conjunto adecuado de procedimientos para el etiquetado de

			la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
		GSI04.A06	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización,
		GSI04.A07	Se deben implementar procedimientos para la gestión de medios removibles de acuerdo con el esquema de clasificación adoptado por la organización.
		GSI04.A08	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
		GSI04.A09	Los medios que contienen información, se deben proteger contra accesos no autorizados, uso indebido o corrupción durante el transporte.
GSI05	Control de Acceso	GSI05.A01	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
		GSI05.A02	Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
		GSI05.A03	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
		GSI05.A04	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
		GSI05.A05	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
		GSI05.A06	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
		GSI05.A07	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
		GSI05.A08	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
		GSI05.A09	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
		GSI05.A10	El acceso a la información y a las funciones de los sistemas

			de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
		GSI05.A11	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
		GSI05.A12	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
		GSI05.A13	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
		GSI05.A14	Se debe restringir el acceso a los códigos fuente de los programas.
GSI06	Criptografía	GSI06.A01	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
		GSI06.A02	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
GSI07	Gestión de la Seguridad Física y del Entorno	GSI07.A01	Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.
		GSI07.A02	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
		GSI07.A03	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
		GSI07.A04	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
		GSI07.A05	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.
		GSI07.A06	Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
		GSI07.A07	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
		GSI07.A08	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.

		GSI07.A09	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debe estar protegido contra interceptación, interferencia o daño.
		GSI07.A10	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
		GSI07.A11	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
		GSI07.A12	Se debe aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
		GSI07.A13	Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reuso.
		GSI07.A14	Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.
		GSI07.A15	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
GSI08	Gestión de seguridad en las operaciones	GSI08.A01	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.
		GSI08.A02	Se debe controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
		GSI08.A03	Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
		GSI08.A04	Se debe separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
		GSI08.A05	Se debe implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
		GSI08.A06	Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de

			respaldo aceptada.
		GSI08.A07	Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
		GSI08.A08	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
		GSI08.A09	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
		GSI08.A10	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
		GSI08.A11	Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.
		GSI08.A12	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
		GSI08.A13	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.
		GSI08.A14	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se debe planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
GSI09	Gestión de seguridad de las Comunicaciones	GSI09.A01	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
		GSI09.A02	Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
		GSI09.A03	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
		GSI09.A04	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
		GSI09.A05	Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes

			externas.
		GSI09.A06	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
		GSI09.A07	Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
		GSI10.A06	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
		GSI10.A07	Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

7.3.3.4 GESTIÓN DE LA ARQUITECTURA EMPRESARIAL, ADQUISICIÓN Y SOPORTE DE TI

Objetivo: Administrar la infraestructura, Portafolio de servicios de TI y definir el Plan de Continuidad de la Información

Id	Proceso	Id Actividad	Actividad
IAS01	Orientar la gestión de Los Recursos	IAS01.A01	Comunicar e impulsar la adopción de las estrategias de gestión de recursos, principios y acordados en el plan de recursos y las estrategias de arquitectura empresarial.
		IAS01.A02	Definir los objetivos clave, medidas y métricas para la gestión de recursos.
		IAS01.A03	Alinear la gestión de recursos con la planificación financiera y de recursos humanos de la empresa.
IAS02	Gestión del Portafolio de Servicios de TI	IAS02.A01	Validar las inversiones TI y los servicios actuales esté alineado con la visión de la empresa, los principios de la empresa, los objetivos estratégicos y los objetivos, la visión arquitectura empresarial y las prioridades.
		IAS02.A02	Identificar las grandes categorías de sistemas de información, aplicaciones, datos, servicios de TI, infraestructura de TI, activos, recursos, habilidades, prácticas, controles y relaciones necesarias para apoyar la estrategia de la empresa.

		IAS02.A03	Definir el portafolio de servicios de TI necesarios para apoyar la estrategia de la empresa, en la cual se contemplen la optimización de recursos, generando valor agregado y asegurando el retorno de la inversión.
IAS03	Gestionar la Continuidad	IAS03.A01	Identificar los procesos empresariales internos y externalizados, y actividades de servicio que son críticos para las operaciones de la empresa o necesario para cumplir obligaciones legales y / o contractuales, así mismo lo requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas.
		IAS03.A02	Definir y documentar los objetivos y el alcance mínimo acordado de la política de continuidad del negocio y la necesidad de integrar la planificación de la continuidad en la cultura de la empresa.
		IAS03.A03	Definir y documentar un plan de continuidad que contemple los activos críticos, el análisis de impacto (BIA), tiempos mínimos de recuperación, duración aceptable y duración máxima de recuperación, requerimientos, recursos y responsables de los activos de información.
		IAS03.A04	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa,
IAS04	Revisar, Mantener y Mejorar el Plan de Continuidad	IAS04.A01	Revisar el plan de continuidad y su capacidad sobre una base regular contra los supuestos realizados y los objetivos operativos y estratégicos de negocio actual.
		IAS04.A02	Considerar si puede ser necesaria una revisión del análisis de impacto en el negocio, dependiendo de la naturaleza del cambio.
		IAS04.A03	Recomendar y comunicar los cambios en las políticas, planes, procedimientos, la infraestructura, los roles y responsabilidades para la aprobación de la dirección y procesamiento a través del proceso de gestión del cambio.
		IAS04.A04	Revisar el plan de continuidad de forma regular para considerar el impacto de los cambios nuevos o mayores a: organización empresarial, procesos de negocio, los acuerdos de subcontratación, tecnologías, infraestructura, sistemas operativos y sistemas de aplicación.
IAS05	Gestión de proveedores	IAS05.A01	Asegurar la protección de los activos de la entidad que sean accesibles para los proveedores
		IAS05.A02	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores

IAS06	Gestión de Incidentes	IAS06.A01	Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
		IAS06.A02	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
		IAS06.A03	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
		IAS06.A04	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
		IAS06.A05	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
		IAS06.A06	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.
		IAS06.A07	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
IAS07	Gestión de seguridad en la adquisición, desarrollo y mantenimiento de sistemas.	IAS07.A01	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
		IAS07.A02	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
		IAS07.A03	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
		IAS07.A04	Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
		IAS07.A05	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.

		IAS07.A06	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
		IAS07.A07	Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
		IAS07.A08	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
		IAS07.A09	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
		IAS07.A10	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
		IAS07.A11	Durante el desarrollo se debe llevar a cabo pruebas de funcionalidad de la seguridad.
		IAS07.A12	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se debe establecer programas de prueba para aceptación y criterios de aceptación relacionados.
		IAS07.A13	Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.
IAS08	Gestión financiera	IAS08.01	Definir procesos, entradas y salidas y responsabilidades de manera alineada con las políticas y el enfoque empresariales de presupuesto y contabilización de costes para manejar sistemáticamente el presupuesto y asignación de costes de TI; catalizar estimaciones de costes y beneficios de TI justos, trasparentes, repetibles y comparables y usarlos como dato de entrada a la cartera de programas de negocio habilitados por las TI; y asegurarse de que se mantienen los presupuestos y costes de las carteras de servicios y activos de TI.
		IAS08.02	Definir la forma de analizar, informar (a quién y cómo), y utilizar el control presupuestario y los procesos de gestión de beneficios.
		IAS08.03	Implementar un presupuesto formal de TI, incluyendo todos los costes de TI esperados de los programas habilitados por las TI, servicios de TI y activos de TI según las indicaciones de la estrategia, programas y carteras.
		IAS08.04	registrar, mantener y comunicar el presupuesto actual de TI, incluidos los gastos comprometidos y los gastos corrientes,

			teniendo en cuenta los proyectos de TI registrados en las carteras de inversiones habilitadas por TI y la operación y el mantenimiento de las carteras de activos y servicios
		IAS08.05	Alinear los presupuestos y servicios de TI a la infraestructura de TI, procesos empresariales, y a los propietarios que los utilizan.
		IAS08.06	A intervalos regulares, y especialmente cuando se recortan los presupuestos debido a limitaciones financieras, identificar formas de optimizar los costes e introducir eficiencia sin poner en peligro los servicios.
		IAS08.A12	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se debe establecer programas de prueba para aceptación y criterios de aceptación relacionados.
		IAS08.A13	Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.

7.3.3.5 GESTIÓN DEL TALENTO HUMANO, APRENDIZAJE Y DESARROLLO - TAD

Objetivo: Gestionar, evaluar y mantener el Talento Humano del área de TI, la transferencia de conocimientos y el cambio organizacional.

Id	Proceso	Id Actividad	Actividad
TAD01	Gestión de Recursos Humanos	TAD01.A01	Definir las habilidades y competencias necesarias y disponibles actualmente tanto de recursos internos como externos para lograr los objetivos de empresa, de TI y de procesos.
		TAD01.A02	Proporcionar una planificación formal de la carrera y desarrollo profesional para fomentar el desarrollo de competencias, oportunidades de progreso personal y una menor dependencia de personas clave.
		TAD01.A03	Desarrollar y ejecutar programas de formación basados en los requisitos organizativos y de procesos, incluidos los requisitos sobre conocimiento empresarial, control interno, conducta ética y seguridad.
		TAD01.A04	Establecer los objetivos individuales alineados con los objetivos de los procesos relevantes, de modo que exista una clara contribución a los objetivos de TI y empresariales.

			Basar las metas en objetivos SMART (específicos, medibles, realizables, pertinentes y de duración determinada) que reflejen las competencias básicas, los valores empresariales y las habilidades necesarias para la(s) función(es).
		TAD01.A05	Realizar la evaluación de desempeño del Recursos Humano, proporcionando la retroalimentación oportuna sobre el desempeño frente a las metas del individuo.
TAD02	Cultivar y facilitar una cultura de intercambio de conocimientos	TAD01.A01	Comunicar proactivamente el valor del conocimiento para impulsar la creación, uso, reutilización y compartición de conocimiento.
		TAD01.A02	Crear un entorno, herramientas y elementos que den soporte a la compartición y transferencia de conocimientos.
		TAD01.A03	Integrar prácticas de gestión del conocimiento en otros procesos de TI.
		TAD01.A04	Identificar usuarios potenciales de conocimiento, incluyendo propietarios de información que pueden necesitar contribuir y aprobar conocimiento. Obtener requisitos de conocimiento y fuentes de información de los usuarios identificados.
		TAD01.A05	Educar y entrenar a los usuarios en el conocimiento disponible, en el acceso al conocimiento y en el uso de herramientas de acceso al conocimiento.
TAD 03	Gestión del Cambio Organizacional	TAD 03.A01	Evaluar el alcance y el impacto del cambio divisado, las diferentes partes interesadas que se verán afectadas, la naturaleza del impacto y la involucración necesaria por cada grupo de partes interesadas y la disposición y habilidad actual para adoptar el cambio.
		TAD 03.A02	Proveer un liderazgo visible por parte de la alta dirección para establecer la dirección y alinear, motivar e inspirar a las partes interesadas en desear el cambio.
		TAD03.A03	Identificar estructuras organizativas compatibles con la visión; si fuera necesario, realizar cambios para asegurar el alineamiento.
		TAD03.A04	Planificar las necesidades de formación del personal para desarrollar las habilidades y actitudes adecuadas para que se sientan facultados.
		TAD03.A05	Alinear los procesos de RRHH y sistemas de medición (p. ej., evaluación del desempeño, decisiones de compensación, decisiones de promoción, reclutamiento y contratación) para dar soporte a la visión.

		TAD03.A06	Llevar a cabo auditorías de cumplimiento para identificar las causas raíz de una baja adopción de los cambios y recomendar acciones correctivas.
		TAD03.A07	Proporcionar tutoría, formación, entrenamiento y transferencia de conocimiento al personal nuevo para mantener los cambios.
		TAD03.A08	Captar lecciones aprendidas sobre la implementación de los cambios y divulgar este conocimiento en toda la empresa.

7.3.3.6 CONTROL, EVALUACIÓN Y MEJORA - CEM

Objetivo: Realizar el control, la evaluación y la mejora de los procesos de TI, a través de la ejecución de auditorías Internas y/o Externas

Id	Proceso	Id Actividad	Actividad
CEM01	Evaluar el Sistema de Control Interno	CEM01.A01	Realizar actividades de vigilancia y evaluación del control interno sobre la base de las normas de gobierno de la organización y los marcos aceptados por la industria y prácticas. Incluir el monitoreo y la evaluación de la eficiencia y efectividad de los exámenes de control de gestión.
		CEM01.A02	Realizar auditorías Internas para supervisar los controles determinados, el cumplimiento de los procesos internos y regulaciones externas
		CEM01.A03	Mantener el sistema de control interno de TI, teniendo en cuenta los cambios en curso en los negocios y los riesgos de TI, el entorno de control de la organización, negocios relevantes y los procesos de TI y los riesgos de TI. Si existen lagunas, evaluar y recomendar cambios.
		CEM01.A04	Identificar, reportar y registrar excepciones de los controles, y asignar la responsabilidad de resolverlos y comunicación de los resultados.
		CEM01.A05	Identificar, iniciar, controlar y aplicar las medidas correctivas derivadas de las evaluaciones de control y presentación de informes.
CEM02	Cumplimiento de Requisitos Legales	CEM02.A01	Identificar y evaluar todos los posibles requisitos de cumplimiento y el impacto en las actividades de TI en áreas tales como el flujo de datos, privacidad, controles internos, informes financieros, las regulaciones específicas de la industria, la propiedad intelectual,

			la salud y la seguridad.
		CEM02.A02	Evaluar el impacto de los requisitos legales y reglamentarios relacionados con la TI en los contratos de terceros relacionados con las operaciones de TI, proveedores de servicios y socios comerciales de negocios.
		CEM02.A03	Revisar periódicamente y ajustar las políticas, principios, normas, procedimientos y metodologías para determinar su eficacia para garantizar el cumplimiento necesario y abordar el riesgo de la empresa de expertos internos y externos, según sea necesario.

7.4 ROLES Y RESPONSABILIDADES

Las empresas de mejor desempeño han establecido varios niveles de gobierno empresarial de TI con funciones y responsabilidades claras, grupos de trabajo en diferentes niveles organizacionales dichos grupos tienen como objetivo construir la visión de largo plazo, asegurar que se cumplan los compromisos adquiridos y que se logre el retorno de inversión. Gad J Selig.

Para el caso de estudio del presente proyecto contraloría territorial de la Guajira se propone una estructura organizacional que define los roles que involucran a la Dirección y comités de gobierno y gestión de TI y del negocio.

CONTRALOR TERRITORIAL (CEO)

El papel del CEO y el equipo ejecutivo de administración es compleja y requiere un equilibrio entre mantener el crecimiento y la rentabilidad al tiempo que optimiza la eficacia organizativa y cumplir con la creciente y confusa serie de requisitos reglamentarios.

- ✓ Definir y aprobar las metas corporativas de la entidad.
- ✓ Aprobar las políticas institucionales en materia de seguridad, riesgos y directrices relacionadas con las Tecnologías de la Información y la comunicación.

DIRECTOR DE TI (CIO)

Los CIO (Chief Information Officer) son los líderes de la gestión estratégica de Tecnologías de Información, encargados de planificar, organizar, coordinar, gestionar y controlar la estrategia de uso y apropiación de TI, y todo lo que conlleva esta tarea. Por tanto un CIO dentro de la Estrategia TI colombiana:

- ✓ Construir plan estratégico para TI
- ✓ Construir planes tácticos para TI
- ✓ Analizar portafolios de programas, administrar portafolios de servicios y proyectos.
- ✓ Establecer estructura organizacional de TI, incluyendo comités y relaciones a los interesados y proveedores
- ✓ Diseñar marco de trabajo para los procesos de TI
- ✓ Establecer e implementar roles y responsabilidades de TI, incluida la supervisión y segregación de funciones
- ✓ Establecer y mantener proceso presupuestal de TI
- ✓ Identificar, comunicar y monitorear la inversión, costo y valor de TI para el negocio
- ✓ Elaborar y mantener Políticas de TI
- ✓ Comunicar el marco de control y los objetivos y dirección de TI
- ✓ Identificar las habilidades de TI
- ✓ Realizar comparaciones con empresas del sector sobre descripciones de puestos de trabajo, rango de salarios y desempeño del personal
- ✓ Ejecutar las políticas y procedimientos relevantes de Recursos Humanos para TI (reclutar, contratar, compensar, entrenar, evaluar, promover y terminar contratos)

- ✓ Identificar eventos asociados con objetivos del negocio y algunos que están orientados a TI
- ✓ Definir las políticas de seguridad y de administración de riesgos del área de TI, de acuerdo a las políticas institucionales.

DIRECTOR FINANCIERO (CFO):

- ✓ Dar mantenimiento al portafolio de programas de inversión
- ✓ Determinar la alineación de la administración de riesgos
- ✓ Aprobar y asegurar fondos para planes de acción de riesgos
- ✓ Mantener informada a la alta gerencia del desempeño de las inversiones y garantizar el adecuado tratamiento a los riesgos que resulten del desarrollo del ejercicio

RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

Tiene a su cargo liderar el proyecto de implementación el Sistema de gestión de seguridad de la información en la entidad,

- ✓ Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo
- ✓ Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.
- ✓ Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.

- ✓ Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.
- ✓ Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos.
- ✓ Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo
- ✓ Encarrilar el proyecto hacia el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la entidad.
- ✓ Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.

RESPONSABLE DE LA GESTIÓN DEL RIESGO

Se encarga de:

- ✓ Valorar/Evaluar riesgos asociados a los eventos
- ✓ Evaluar y seleccionar la respuesta a los riesgos
- ✓ Definir el plan de tratamiento de Riesgos.
- ✓ Evaluar, Mantener y mejorar el plan de tratamiento de riesgos, de acuerdo a los cambios organizacionales

RESPONSABLE DE INFRAESTRUCTURA

Ejecutar los programas de infraestructura de manera oportuna, con calidad y en el marco del presupuesto otorgado y de las normas legales sobre la materia, velando por su correcta ejecución y culminación.

- ✓ Asegurar el funcionamiento integral de la infraestructura tecnológica (comunicaciones, redes de comunicaciones, backups, servidores, telefonía) de la empresa.
- ✓ Asegurar que los proveedores cumplan con mantener un alto nivel de servicio en las áreas de su responsabilidad: plataforma tecnológica (servidores, almacenamiento), comunicaciones, telefonía e infraestructura (cableado de datos y eléctrico de redes de comunicaciones).
- ✓ Planificar y obtener la homogeneidad de equipos y de software base con el fin de maximizar la disponibilidad de los servicios de información.
- ✓ Planificar los tiempos de atención de fallas y desperfectos por parte de los proveedores y controlar el cumplimiento de los mismos.
- ✓ Gestionar el proceso de Arrendamiento Operativo de la Infraestructura Tecnológica de la compañía (PC's, Servidores, RDT's, Impresoras, Periféricos, Redes LAN, WAN, WiFi)

Teniendo en cuenta lo anterior, a continuación se define la matriz de responsabilidades de cada uno de los roles en los diferentes procesos, para ellos utilizaremos la matriz RACI que indica lo siguiente:

R (Responsible): es quien ejecuta una tarea. Su función es "HACER".

A (Accountable): es quien vela porque la tarea se cumpla, aún sin tener que ejecutarla en persona. Su función es "HACER HACER".

C (Consulted): indica que una persona o área debe ser consultada respecto de la realización de una tarea.

I (Informed): indica que una persona o área debe ser informada respecto de la realización de una tarea.

MATRIZ RACI								
DOMINIO	PROCESO	CONTRALOR TERRITORIAL	DIRECTOR DE TI	DIRECTOR FINANCIERO	RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN	RESPONSABLE DE RIESGOS	RESPONSABLE DE INFRAESTRUCTURA	RESPONSABLE DE MEDICIÓN Y CONTROL
PDE	PDE01	A	R	C	C	C	C	I
	PDE02	A	R	C	C	C	C	I
	PDE03	A	R	C	C	C	C	I
	PDE04	R	C	C	C	C	C	A
	PDE05	A	C	C	C	C	C	R
	PDE06	A	C	C	C	C	C	R
RTI	RTI01	A	A	C	C	R	I	I
	RTI02	A	A	C	C	R	C	I
	RTI03	A	A	C	C	R	C	I
	RTI04	A	A	C	C	C	C	R
GSI	GSI01	A	A	C	R	C	C	I
	GSI02	A	A	C	C	R	C	I
	GSI03	A	A	C	C	C	I	R
	GSI04	A	R	C	C	I	R	I
	GSI05	A	R	R	C	I	R	
	GSI06	A	A		R		R	
	GSI07	A	A		R			
	GSI08	A	A		R	C	R	
	GSI09	A	R	I	R	C	R	I
	GSI10	A	A		R	C	R	

IAS	IAS01	A	R	C	I	I	I	I
	IAS02	A	R	C	C	C	R	I
	IAS03	A	A	I	C	C	R	I
	IAS04	A	R	I	I	I	R	I
	IAS05	A	R	C	C	C	R	I
	IAS06	A	A	I	R	R	R	I
	IAS07	A	R	I	R	C	R	I
	IAS08	A	C	R	C	C	C	I
TAD	TAD01	A	R	I	I	I	I	I
	TAD02	A	R	I	C	C	C	I
	TAD03	A	R	I	C	C	R	I
CEM	CEM01	A	C	C	C	C	C	R
	CEM02	A	C	C	C	C	C	R

7.5 INDICADORES DE DESEMPEÑO

MÉTRICAS DE TI		
PROCESO	**ID PROCESO**	**MÉTRICAS ASOCIADAS**
PLANEACIÓN Y DIRECCIÓN ESTRATÉGICA DE TI	**PDE**	Porcentaje de metas estratégicas y requerimientos corporativos apoyados por metas TI estratégicas
		Nivel de satisfacción del usuario del negocio con la calidad y la puntualidad (o disponibilidad) de la información de gestión
		Porcentaje de los roles de la gestión ejecutiva con responsabilidades claramente definidas para las decisiones de TI
GESTIÓN DE RIESGOS DE TI	**RTI**	Porcentaje de procesos TI de negocio críticos, servicios TI y programas de negocio habilitados por TI cubiertos por evaluaciones de riesgo
		Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos
GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	**GSI**	Número de incidentes de seguridad causantes de pérdidas financieras, interrupción del negocio o vergüenza pública
		Número de incidentes de seguridad causados por la no observancia del plan de seguridad
GESTIÓN DE LA ARQUITECTURA EMPRESARIAL, ADQUISICIÓN Y SOPORTE DE TI	**IAS**	Nivel de satisfacción de los interesados con el alcance del portafolio de programas y servicios planificado
		Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios TI
		Número de interrupciones del negocio debidas a incidentes en el servicio de TI
GESTIÓN DEL TALENTO HUMANO, APRENDIZAJE Y DESARROLLO	**TAD**	Porcentaje del personal cuyas habilidades TI son suficientes para las competencias requeridas para su función
		Porcentaje de rotación del personal
		Número de usuarios formados en el uso y compartición de conocimiento
		Porcentaje de funcionarios a los que se les aplica evaluación de desempeño
		Nivel de satisfacción de las partes interesadas con los niveles de experiencia e ideas de la innovación TI
CONTROL, EVALUACIÓN Y MEJORA	**CEM**	Coste de incumplimientos TI, incluyendo acuerdos y sanciones e impacto en pérdida de reputación
		Número de incidentes relacionados con el incumplimiento de políticas.

8 MODELO DE MADUREZ

El siguiente esquema permite identificar el nivel de madurez en el que se encuentran las entidades, midiendo la brecha entre el nivel actual de la entidad el nivel optimizado, está basado en la norma ISO 15504, en cuya parte 7, se definen los requisitos mínimos para realizar una evaluación de determinación de la madurez de una organización, en la cual se manejan seis niveles:

ESCALA DE MEDICIÓN DE LOS PROCESOS			
NIVEL	**DESCRIPCIÓN**	**DETALLE**	**CALIFICACIÓN**
Nivel 0	Incompleto	El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.	0
Nivel 1	Ejecutado	La organización implementa y alcanza los objetivos del proceso.	1
Nivel 2	Gestionado	El proceso ejecutado del nivel 1 es implementado de forma gestionada (planificado, supervisado y ajustado) y sus resultados son debidamente establecidos, controlados y mantenidos.	2
Nivel 3	Establecido	El proceso gestionado del nivel 2 se implementa usando un proceso definido que es capaz de alcanzar sus objetivos.	3
Nivel 4	Predecible	El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso	4
Nivel 5	Optimizado	El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con las metas empresariales presentes y futuros.	5

Tabla 7: Escala de Medición de los procesos según ISO 15504.
Fuente: Elaboración Propia, basado en la norma ISO 15504

9 GUÍA DE IMPLEMENTACIÓN

Para lograr la implementación del modelo propuesto de manera tal que sea aplicable a la entidad Contraloría General del Departamento de La Guajira, así como para las demás entidades del sector, es necesario definir una guía que muestre el paso a paso de esta implementación, como parte de un ciclo de vida de mejora continua, basado en el modelo de implantación de COBIT 5, planteada por el IT Governance Institute, y adaptada para el caso de las entidades bancarias[4], el cual consta de siete fases:

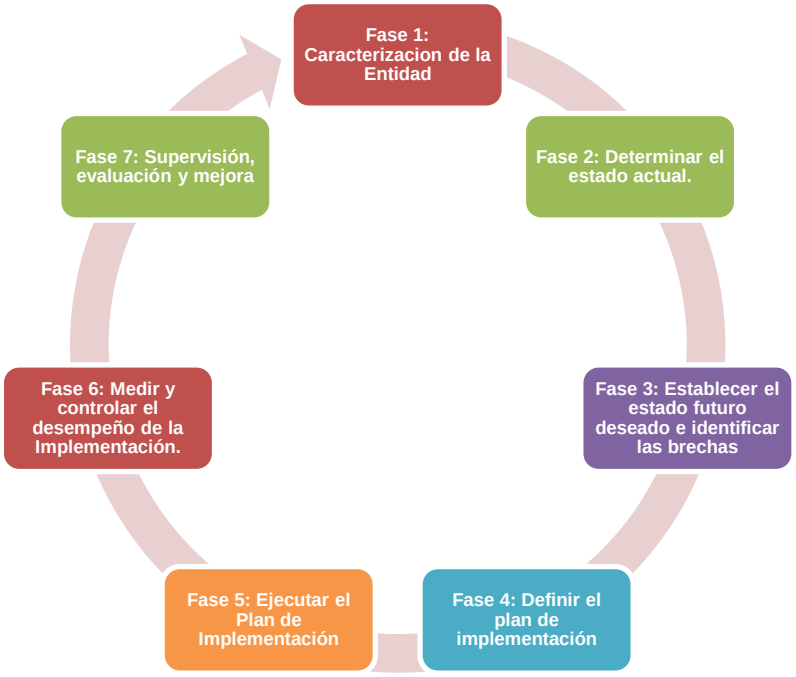


Figura 15: Proceso Guía de Implementación

Fuente: Elaboración Propia

Esta guía tiene objetivos lo siguiente:

1. Considerar el Contexto Institucional.

[4] La guía propuesta es una adaptación de la tesis de maestría, Modelo y guía para la implementación de Gobierno de TI en Entidades Bancarias de Colombia. Desarrollada por María Helena Correa y Breyner Alexander Parra Rojas, (ICESI, 2012).

2. Crear el entorno apropiado.
3. Reconocer los puntos débiles y sus eventos desencadenantes.
4. Facilitar el cambio.
5. Enfoque de ciclo de vida, lo que determina la supervisión, el mantenimiento y la mejora del sistema de gobierno.

FASE 1: CARACTERIZACIÓN DE LA ENTIDAD

En esta fase se debe realizar la caracterización organizacional en relación a los procesos que maneja, determinar su misión, visión, estructura organizacional, productos y servicios institucionales.

En esta fase es importante que la alta dirección manifieste el deseo del cambio, reconociendo las necesidades actuales de la entidad.

Actividades:

1. Realizar la caracterización de la entidad.
2. Identificar la estructura organizacional actual y los servicios.

FASE 2: DETERMINAR EL ESTADO ACTUAL.

En esta fase se debe hacer una evaluación de las fortalezas, debilidades, oportunidades y amenazas de la entidad y su entorno, se debe definir el equipo de implementación responsable de la misma y hacer un análisis del estado actual de la entidad, en referencia al gobierno y gestión de TI.

Actividades:

1. Realizar una matriz DOFA, donde se identifican las debilidades y fortalezas de la entidad, así mismo las oportunidades y amenazas del entorno, que faciliten o dificulten la gestión TI en la entidad.

2. Determinar el nivel de madurez de los procesos definidos en el modelo de Gobierno y Gestión propuesto.

FASE 3: ESTABLECER EL ESTADO FUTURO DESEADO E IDENTIFICAR LAS BRECHAS.

Determinar el estado del futuro deseado, del nivel de madurez de Gobierno de TI, definiendo a su vez una hoja de ruta de implementación, priorizando aquellas iniciativas que son más fáciles de conseguir y aquellas que podrían proporcionar los mayores beneficios.

Actividades:

1. Proponer la estructura organizacional y de procesos pertinente para el gobierno de TI.
2. Determinar el Nivel de Madurez deseado de los procesos de TI.
3. Identificar las brechas en los procesos a considerar en la fase de implementación del Modelo de Gobierno y Gestión de TI.

FASE 4: DEFINIR EL PLAN DE IMPLEMENTACIÓN

En esta fase se debe establecer el plan de implementación de los proyectos priorizados en la fase anterior, de acuerdo a las brechas definidas y el nivel de importancia.

Actividades:

1. Definir, de acuerdo a las brechas existentes encontradas, cuáles de ellas serán cerradas y cuales solo quedaran planteadas para implementar en un futuro.
2. Identificar en el modelo propuesto y según las brechas a cerrar, los procesos necesarios para alcanzar los objetivos.

3. Convertir los procesos elegidos en proyectos, los cuales deberán tener sus responsables asignados, metas, recursos y cronograma a seguir.

4. Definir el orden en el cual se ejecutarán los proyectos establecidos.

FASE 5: EJECUTAR EL PLAN DE IMPLEMENTACIÓN

En esta fase se deben ejecutar las estrategias definidas en el plan determinado en la fase anterior.

Actividades:

1. Implementar cada proyecto en el orden establecido en la fase anterior

2. Para cada proyecto, gestionar los recursos económicos, físicos y humanos necesarios; además de cualquier tipo de recurso necesario adicional para llevar a cabo cada proyecto

3. Realizar las actividades necesarias en cada proyecto para dar cumplimiento al mismo en los tiempos planteados en cada cronograma

4. Una vez terminado cada proyecto, realizar pruebas y realizar el cierre del mismo.

FASE 6: MEDIR Y CONTROLAR EL DESEMPEÑO DE LA IMPLEMENTACIÓN.

La fase 6 se focaliza en la supervisión de la consecución de los beneficios esperados, a través de la medición de los indicadores, y establecer la supervisión empleando las metas y métricas de COBIT para asegurar que se consigue y mantiene la alineación con el negocio y que el rendimiento puede ser medido.

Actividades:

1. Medición de los indicadores establecidos para los procesos, y controlar su desempeño.

2. Informar de manera periódica la medición efectuada a los procesos a la alta dirección y las partes interesadas.

FASE 7: SUPERVISIÓN, EVALUACIÓN Y MEJORA

Durante la fase 7, se revisa el éxito global de la iniciativa, se identifican requisitos adicionales para el gobierno o la gestión de la TI empresarial y se refuerza la necesidad de mejora continua.

Actividades:

1. Supervisar el cumplimiento de metas de los indicadores de los procesos.

2. Hacer una revisión sobre la efectividad de los resultados.

3. Determinar acciones de mejoramiento a los procesos

10 CASO DE ESTUDIO: CONTRALORÍA GENERAL DEL DEPARTAMENTO DE LA GUAJIRA

10.1 CARACTERIZACIÓN

La Contraloría territorial del Departamento de La Guajira (CGDG), que es el ente encargado de ejercer la oportuna gestión fiscal a los entes territoriales del departamento, en articulación con las entidades afines, promoviendo la participación ciudadana, el control social y ambiental; para la transparencia y efectividad en el manejo de los recursos públicos e inversión social, en esta región de la República de Colombia.

Esta Institución de control fiscal territorial cuenta con una planta de personal de 22 funcionarios distribuidos en ocho dependencias como se aprecia en la Figura 9, Tiene 49 años de antigüedad (1967-2016), y hacia el 2019, se visiona como un órgano de control visible con mayor cobertura en la vigilancia de los recursos públicos, generando confianza en la comunidad como resultado el ejercicio del control fiscal.

10.1.1 MISIÓN

Ejercer oportuna gestión fiscal a los entes sujetos de control, en articulación con las entidades afines, promoviendo la participación ciudadana, el control social y ambiental; para la transparencia y efectividad en el manejo de los recurso públicos e inversión social.

10.1.2 VISIÓN

Al 2019, la Contraloría General del Departamento de La Guajira será un órgano de control visible con mayor cobertura en la vigilancia de los recursos públicos, generando confianza en la comunidad como resultado el ejercicio del control fiscal actuación la transparencia, la eficacia y la eficiencia. Y así ser garantes del desarrollo sostenible de nuestro Departamento.

10.1.3 ESTRUCTURA ORGANIZACIONAL

Figura 16: Estructura Organizacional de la Contraloría General del Departamento de La Guajira.
Fuente: Contraloría Departamental de La Guajira

10.2 ESTRUCTURA DE PROCESOS

10.2.1 SISTEMA INTEGRADO DE GESTIÓN DE CALIDAD

El Sistema de Gestión de la Calidad de La Contraloría General del Departamento de la Guajira, tiene un enfoque basado en procesos que busca mejorar continuamente las actividades inherentes a la naturaleza del control fiscal y aumentar la satisfacción de las entidades sujetas a control y de la comunidad en general, mediante el cumplimiento de sus requisitos legales y reglamentarios y los establecidos en las normas NTC GP 1000:2009 e ISO 9001:2008, a través de la identificación e interacción de sus procesos.

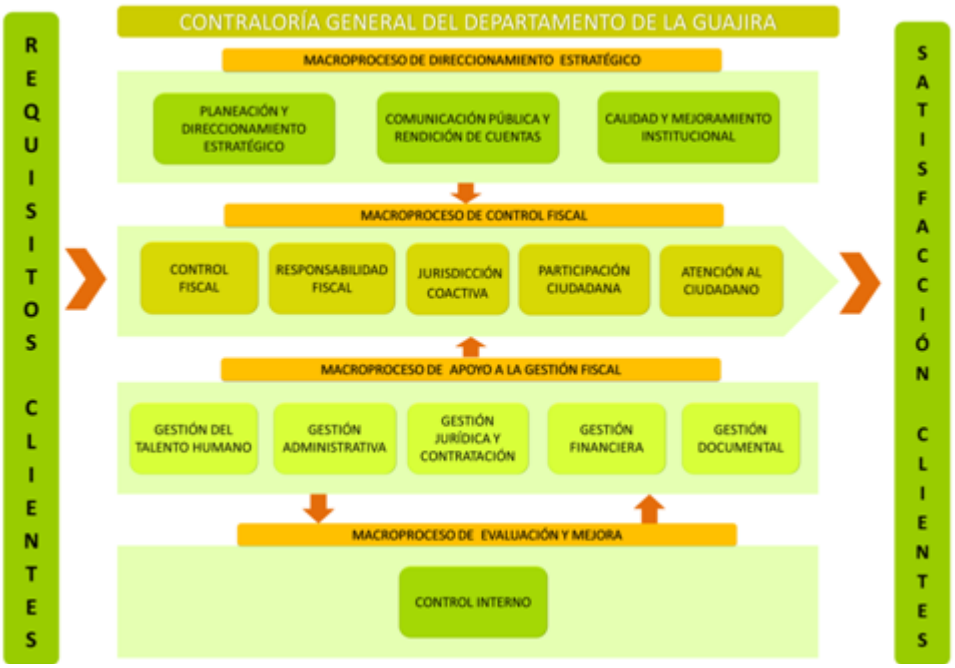


Figura 17: Mapa de procesos Contraloría General del Departamento de La Guajira
Fuente: SGC Contraloría General del Departamento de La Guajira

10.3 HISTORIA

El Departamento de La Guajira fue creado en el año de 1964, mediante la Ley 19 del 10 de noviembre, iniciando su vida jurídica a partir del 1º de julio de 1965, siendo su primer Contralor por decreto; el Doctor JACOBO MÁRQUEZ IGUARAN, durante el lapso comprendido entre junio y noviembre de 1967.

Con base en el numeral 3º del artículo 187 de la anterior Constitución Nacional, la Asamblea Departamento de La Guajira expidió la Ordenanza No. 09 del 8 de noviembre de 1967, por la cual se organiza la Contraloría General del Departamento y se crea el cargo de Contralor. A partir de esa fecha ha tenido 18 contralores departamentales.

Hasta la expedición de la Constitución de 1991, el rol que cumplía la Contraloría General del Departamento de La Guajira, la definía como un organismo cuyas tareas reflejaban un carácter mecánico y pasivo en la aplicación del control previo, la pasividad se manifestaba en el hecho de resaltar el control numérico legal y minimizar el análisis de resultados.

La imagen negativa de la Contraloría se desprendía del carácter pasivo que tenía el control fiscal, cumpliendo por demás el inadecuado papel de coadministrador de la gestión pública, que en muchas oportunidades derivaron en graves cuestionamientos.

La Constitución de 1991, le dio una nueva dimensión al control fiscal, dejando de ser numérico-legal para convertirlo en posterior y selectivo. Con la expedición de la Ley 42 del 26 de enero de 1993, se le introdujo un mayor número de sistemas de evaluación y vigilancia a partir del control financiero, de legalidad, de gestión, de resultados y la evaluación del control interno.
Como complemento de la anterior disposición, las Resoluciones Reglamentarias Nº: 003, 008, 009 y 012 de 1995, por medio de las cuales se adoptaron los manuales para el ejercicio del control financiero, físico, de legalidad, de gestión y valoración de los costos ambientales, respectivamente, la Contraloría General del Departamento, implementó importantes mecanismos de control para la práctica de las auditorias integrales, las cuales se iniciaron el mismo año, con el propósito de evaluar la eficiencia, la eficacia, la economía, la equidad y la valoración de los costos ambientales, en la obtención y aplicación de los recursos públicos. Adicionalmente, mediante la ordenanza 036 expedida el 6 de diciembre de 1995, se le dio luz verde a la estructura orgánica y administrativa de la entidad, dotándola de instrumentos que la facultaron para llevar a cabo con eficiencia y eficacia su función fiscalizadora.

Con la promulgación de la Constitución de 1991, se hace necesario observar la responsabilidad que tienen los funcionarios del Estado de hacer uso racional y eficiente de los recursos públicos, focalizándose hacía el cumplimiento de objetivos prioritarios

de crecimiento económico, social y ambiental de los entes territoriales. En la Carta Política, el control fiscal a la gestión pública pasó de ser previo y perceptivo, a posterior y selectivo. No obstante, el nuevo enfoque del control permitía la aplicación de un control de advertencia o de prevención, el cual fue declarado inexequible por la corte constitucional en sentencia C-103-15.

En tal sentido, con las iniciativas propias de su gestión, la Contraloría General del Departamento de La Guajira, introdujo cambios sustanciales en materia institucional y administrativa, buscando con ello dinamizar procesos de cambio en la gestión pública, que pueden interpretarse como el traslado de la eficacia y la eficiencia de la organización de las empresas de carácter privado, al ámbito de las entidades públicas sin que estas pierdan su naturaleza.

10.4 PRODUCTOS Y SERVICIOS

La Contraloría General del Departamento de la Guajira es un organismo de carácter técnico dotadas de autonomía administrativa, presupuestal y contractual, la cual ejerce la función pública de control fiscal en su respectiva jurisdicción, de acuerdo con los principios, sistemas y procedimientos establecidos en la Constitución y la ley. La Contraloría General del Departamento de La Guajira no tendrá funciones administrativas distintas de las inherentes a su propia organización.

En consideración a lo establecido en los Artículos 268 y 272 del Constitucional primario, y lo contenido en la Ley 330 de 1996 en su Artículo 9° corresponde a la Contraloría General del Departamento de La Guajira:

- ✓ Prescribir, teniendo en cuenta las observaciones de la Contraloría General de la República, los métodos y la forma de rendir cuentas los responsables de manejos de fondos o bienes departamentales y municipales que no tengan Contraloría e

indicar los criterios de evaluación financiera, operativa y de resultados que deberán seguirse.

- ✓ Revisar y fenecer las cuentas que deben llevar los responsables del Erario bajo su control y determinar el grado de eficiencia, eficacia, y economía con que hayan obrado.

- ✓ Llevar un registro de la deuda pública del departamento, de sus entidades descentralizadas y de los municipios que no tengan Contraloría.

- ✓ Exigir informes sobre su gestión fiscal a los servidores públicos del orden departamental o municipal, y a toda persona o entidad pública o privada que administre fondos o bienes del departamento y municipio fiscalizado.

- ✓ Establecer las responsabilidades que deriven de la gestión fiscal, imponer las sanciones pecuniarias que sean del caso, recaudar su monto y ejercer la jurisdicción coactiva sobre los alcances deducidos de la misma.

- ✓ Conceptuar sobre la calidad y eficiencia del control fiscal interno de las entidades y organismos del orden departamental y municipal bajo su control.

- ✓ Presentar a la Asamblea Departamental un informe anual sobre el estado de los recursos naturales y del ambiente.

- ✓ Promover ante las autoridades competentes, las investigaciones penales o disciplinarias contra quienes hayan causado perjuicio a los intereses patrimoniales, departamentales y municipales. La omisión de esta atribución los hará incurrir en causal de mala conducta.

- ✓ Presentar anualmente a la Asamblea Departamental y a los Concejos Municipales, un informe sobre el estado de las finanzas de las entidades el departamento a nivel central y descentralizado, que comprenda el resultado de la evaluación y su

concepto sobre la gestión fiscal de la administración en el manejo dado a los fondos y bienes públicos.

- ✓ Realizar cualquier examen de auditoría, incluido el de los equipos de cómputo o procesamiento electrónico de datos, respecto de los cuales podrá determinar la confiabilidad y suficiencia de los controles establecidos, examinar las condiciones del ambiente de procesamiento y adecuado diseño del soporte lógico.
- ✓ Realizar las visitas, inspecciones e investigaciones que se requieran para el cumplimiento de sus funciones.
- ✓ Evaluar la ejecución de las obras públicas que se adelanten en el departamento.
- ✓ Auditar el balance de la hacienda departamental para ser presentado a la Asamblea Departamental.
- ✓ Remitir mensualmente a la Contraloría General de la República la relación de las personas a quienes se les haya dictado fallo con responsabilidad fiscal, para efectos de incluirlos en el boletín de responsabilidades.

10.5 CLIENTES

Los clientes de las Contraloría General del departamento de La Guajira son:

- ✓ La Asamblea departamental.
- ✓ Las entidades pública de orden departamental, municipal, distrital.
- ✓ Las entidades u organismos privados, o personas naturales que administren o manejen recursos públicos.
- ✓ La Ciudadanía en General.
- ✓ Otros entes de control (Fiscalía, Procuraduría, CGR)

11 ESTADO ACTUAL

11.1 DOFA

DEBILIDADES

A pesar de su visión y misión, así como sus bondades con las cuales cuenta la CGDG para dar cumplimiento a sus importantes y vitales funciones para la administración pública regional, esta entidad presenta una serie de debilidades que hace ineficiente e incluso pueden llegar a obstaculizar gravemente su función pública. Dentro de esas debilidades están:

- No tiene en su estructura orgánica, una dependencia encargada de la Dirección General de Sistemas o un Área de Tecnología de la Información (TI).
- Dentro de su modelo de operación por procesos (estratégicos, misionales o de apoyo), no tienen definidos procesos ni procedimientos del área de TI.
- Cuenta con una infraestructura de hardware (equipos) y de redes obsoleta (data del año 2004) y en mal estado, a la cual no se le hace mantenimiento.
- Existen sistemas de información que dan apoyo a algunos procesos (Rendición de cuentas - Auditorías), que no son utilizados de manera eficiente.
- No se cuenta con estándares de seguridad de información, tanto para

FORTALEZAS

- Existe personal capacitado en el área de sistemas con conocimientos en seguridad de la información y gestión del riesgo.
- Existe un sistema de gestión de calidad sobre el cuál es posible adoptar nuevos procesos para la gestión de TI.
- Existe autonomía administrativa del jefe de la entidad para reformar la planta de personal en caso de ser necesario.

- Existe un sistema de Información robusto que recopila los datos de los entes sujetos de control sobre la gestión financiera y contractual (SIA Contraloría y SIA Observa).

AMENAZAS

- Dependencia financiera de la gestión fiscal de la Gobernación, lo que conlleva al manejo de pocos recursos económicos para las gestión administrativa y operativa.
- Falta de confianza por parte de la ciudadanía en el ejercicio de control fiscal.
- Normatividad que dificulta la captación de recursos de otras fuentes, lo que no permite un cubrimiento mayor en el ejercicio de control fiscal.

OPORTUNIDADES

- Cooperación interinstitucional.
- Existencia de marcos de referencia para la de seguridad de la información y gestión de riesgos aplicables a la entidad.
- Apoyo de Ministerio de las TIC para la implementación de la estrategia de gobierno de TI y seguridad de la Información.

ESTRATEGIAS FO

- Implementación de marcos de referencia con base en las mejores prácticas de seguridad y riesgos (ISO 27001 - ISO31000), aprovechando el conocimiento del recurso humano en sistemas y seguridad de la información, integrándolo al SGC de la entidad, con el apoyo del ministerio TIC.

ESTRATEGIAS DO

- Realizar convenios interinstitucionales para fortalecimiento de la infraestructura tecnológica de la entidad, además de obtener productos de software que utilicen otras contralorías o entes de control, para la optimización de los procesos.

ESTRATEGIA FA

- Aprovechar el uso del sistema de información de rendición de cuentas (SIA Contralorías) y Contratación (SIA Observa), para realizar una labor de vigilancia y ejercicios de auditoría en línea, que conlleve pocos gastos de personal (Comisiones, traslados), por lo que con los mismos recursos se puede hacer la labor más eficiente, quedando espacio y recursos para la promoción social y la visibilidad ante la ciudadanía.

ESTRATEGIA DA

- Constituir en la estructura organizacional actual, el área de Dirección de TI, y el comité de gobierno de TI, como ente encargado de gestionar y gobernar lo correspondiente al uso y apropiación de las nuevas tecnologías de la información

11.2 ESTADO ACTUAL VS ESTADO DESEADO

VALORACIÓN DE NIVEL MADUREZ				
		SITUACIÓN ACTUAL	ESTADO DESEADO	
CÓDIGO	PROCESO	CALIFICACIÓN 1	CALIFICACIÓN 2	GAP
PDE01	Esquema y Alineación del Gobierno de TI	0,00	3	3,00
PDE02	Planeación Estratégica de TI	0,00	3	3,00
PDE03	Informes a las Partes Interesadas	1,67	3	1,33
PDE04	Supervisar la comunicación con las partes interesadas.	0,00	3	3,00
PDE05	Evaluación y Mejora Continua del sistema de gobierno de TI.	0,00	3	3,00
RTI01	Orientar la gestión de Riesgos	0,50	3	2,50

RTI02	Valoración del Riesgo de TI	0,33	3	2,67
RTI03	Tratamiento del Riesgo de TI	0,25	3	2,75
RTI04	Supervisión de la Gestión de Riesgos	0,00	3	3,00
GSI01	Establecer y Documentar el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI)	0,00	3	3,00
GSI02	Supervisar y revisar el SGSI.	0,00	3	3,00
GSI03	Seguridad de los Recursos Humanos	0,33	3	2,67
GSI04	Gestión de Activos	0,33	3	2,67
GSI05	Control de Acceso	0,07	3	2,93
GSI06	Criptografía	0,00	3	3,00
GSI07	Gestión de la Seguridad Física y del Entorno	0,13	3	2,87
GSI08	Gestión de seguridad en las operaciones	0,14	3	2,86
GSI09	Gestión de seguridad de las Comunicaciones	0,00	3	3,00
IAS01	Orientar la gestión de Los Recursos	0,33	3	2,67
IAS02	Gestión del Portafolio de Servicios de TI	0,00	3	3,00
IAS03	Gestionar la Continuidad	0,00	3	3,00
IAS04	Revisar, Mantener y Mejorar el Plan de Continuidad	0,00	3	3,00
IAS05	Gestión de proveedores	0,00	3	3,00
IAS06	Gestión de Incidentes	0,00	3	3,00
IAS07	Gestión de seguridad en la adquisición, desarrollo y mantenimiento de sistemas.	0,00	3	3,00
IAS08	Gestión financiera	0,33	3	2,67
TAD01	Gestión de Recursos Humanos	1,40	3	1,60
TAD02	Cultivar y facilitar una cultura de intercambio de conocimientos	0,00	3	3,00
TAD03	Gestión del Cambio Organizacional	0,00	3	3,00
CEM01	Evaluar el Sistema de Control Interno	1,00	3	2,00
CEM02	Cumplimiento de Requisitos Legales	0,33	3	2,67
		0,2	**3,0**	

Tabla 8: Medición Nivel de Madurez
Fuente. Elaboración Propia.

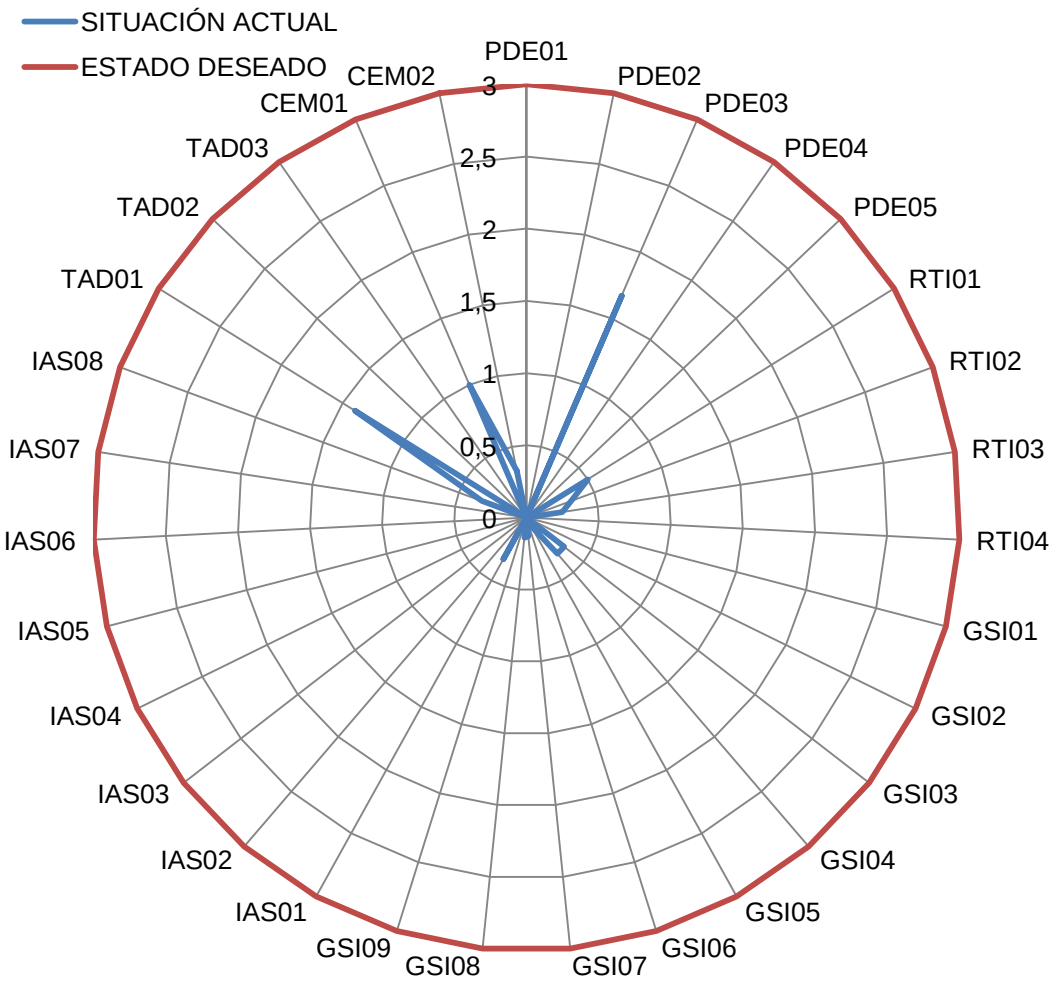


Grafico 1: Nivel de Madurez por Procesos

Fuente: Elaboración Propia

12 FUTURO DESEADO

La siguiente es la estructura organizacional propuesta para a contraloría general del departamento de la guajira, en donde se incluye la Dirección de TI, como ente dinamizador de la estrategia de Gobierno y gestión de TI, de igual forma se establece la estructura de procesos necesarios para esta área, la cual incluyen los más

importantes para desarrollar cada uno de los dominios del modelo de G&G propuesto para la entidad.

12.1 ESTRUCTURA ORGANIZACIONAL PROPUESTA

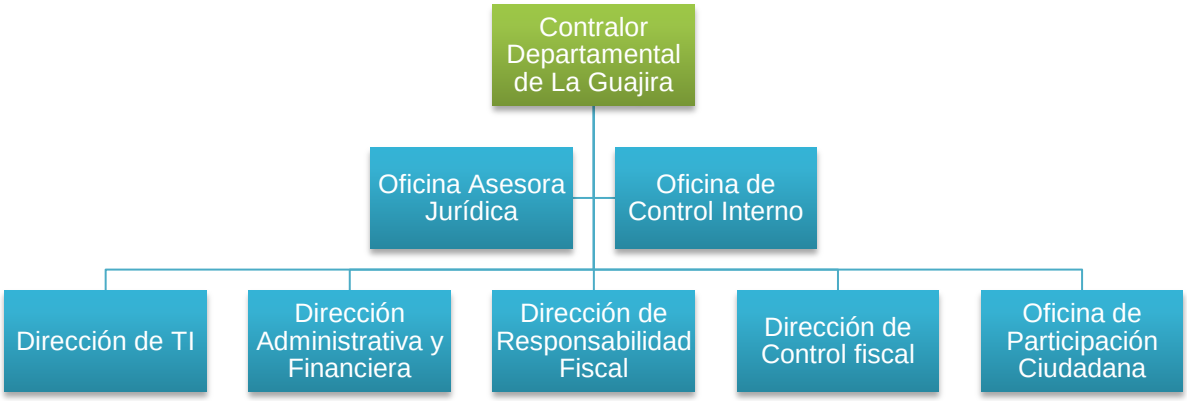


Figura 18: Estructura organizacional propuesta, Contraloría General de La Guajira

Fuente: Elaboración Propia

12.2 MODELO DE GOBIERNO Y GESTIÓN DE TI PROPUESTO, APLICADO A LA CONTRALORÍA GENERAL DEL DEPARTAMENTO DE LA GUAJIRA

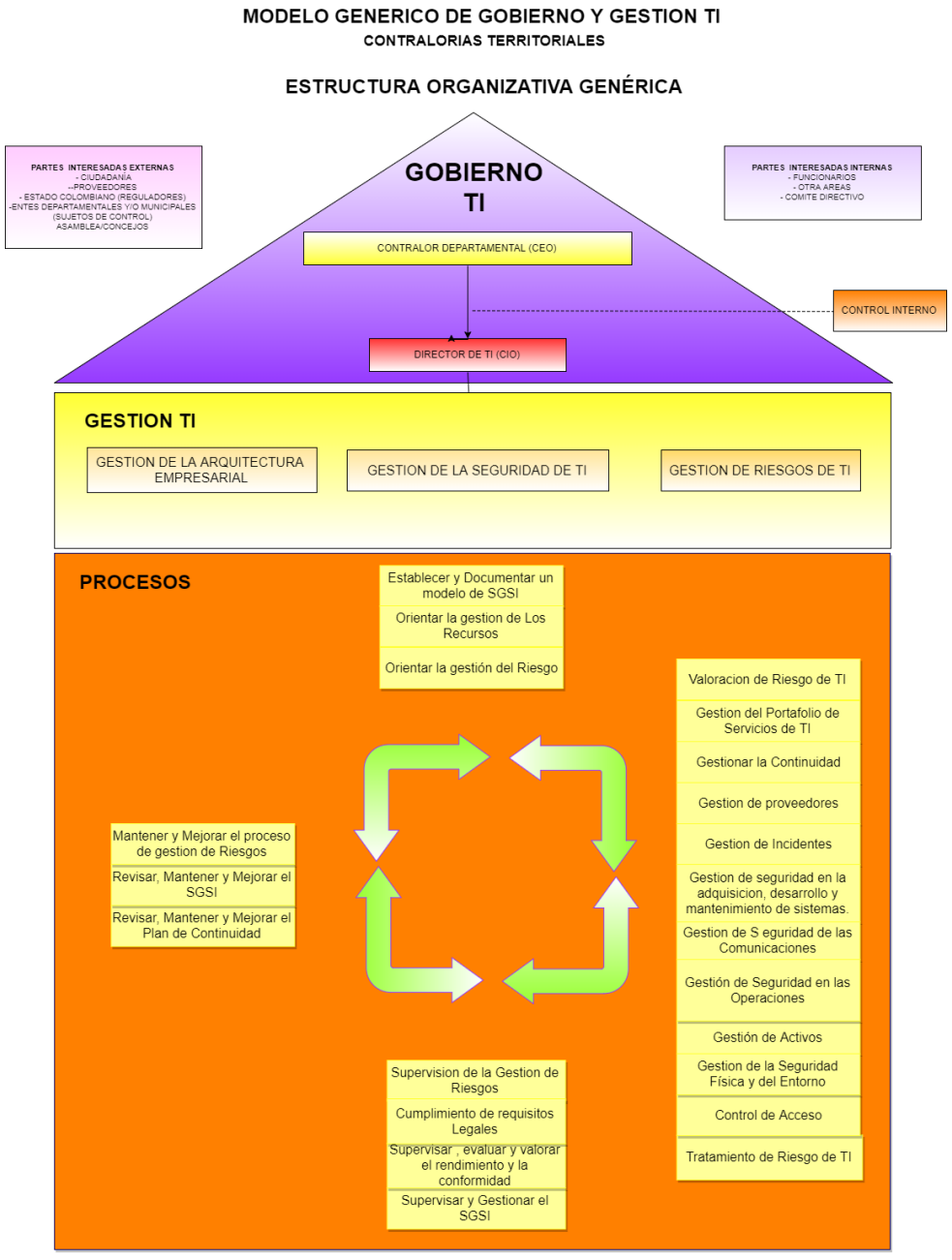


Figura 19: Modelo de Gobierno de Ti para la Contraloría General de La Guajira

Fuente: Elaboración Propia

12.3 ESTRUCTURA DE PROCESOS DEL ÁREA DE TI

A continuación se define el mapa de procesos necesario para la dirección de TI, a través del cual se puedan ejecutar los procesos del modelo de G&G propuesto anteriormente, el cuál puede ser adaptado al Sistema de Gestión de calidad en esta entidad.

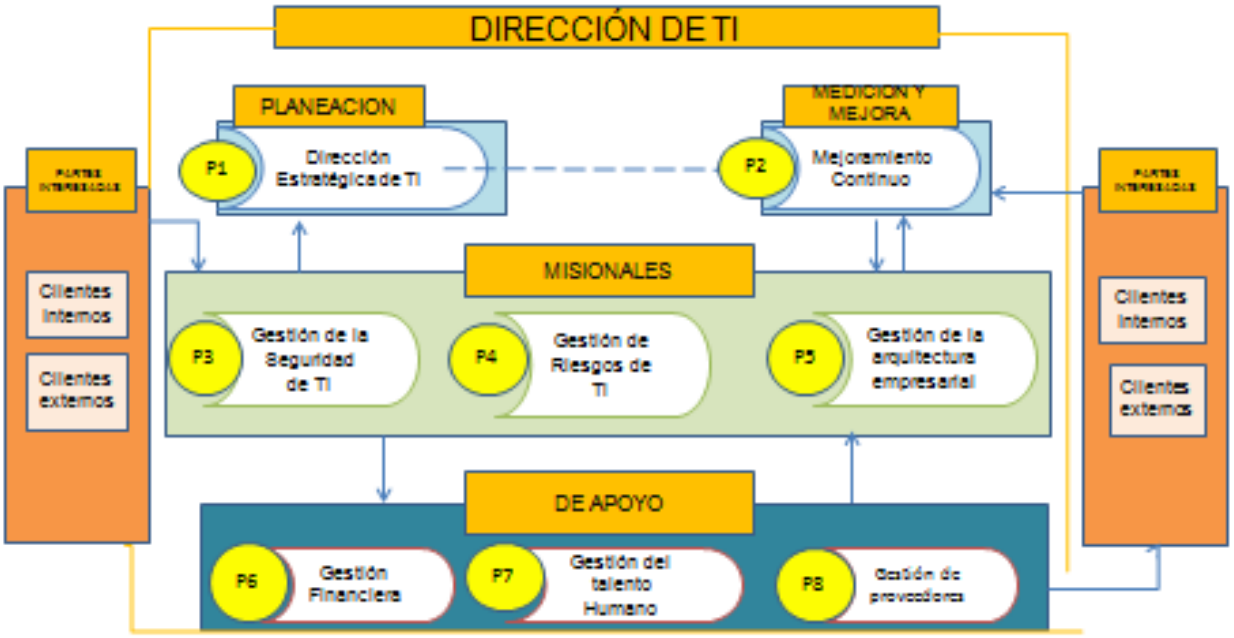


Figura 20: Estructura de procesos de Tecnología Informática para Contraloría Territoriales

Fuente: Elaboración Propia

12.4 IDENTIFICACIÓN DE LAS BRECHAS

En la fase anterior se determinó el estado actual de los procesos de TI de la contraloría general del departamento de la Guajira en referencia al modelo de gobierno y Gestión de TI establecido, teniendo en cuenta el mapa de procesos propuesto anteriormente, se establecerá como prioridad la gestión de la seguridad de la Información, para la implementación del modelo de G&G, el cual contribuye a la consecución de la visión y los objetivos organizacionales como lo son:

Empezando con la visión institucional, que indica lo siguiente:

Al 2019, la Contraloría General del Departamento de La Guajira será un **órgano de control visible con mayor cobertura en la vigilancia de los recursos públicos**, generando **confianza en la comunidad como resultado el ejercicio del control fiscal** actuación la **transparencia, la eficacia y la eficiencia**. Y así ser garantes del desarrollo sostenible de nuestro Departamento.

De allí extraemos las ideas importantes como son:

Para lograr ser un **Órgano de control visible con mayor cobertura en la vigilancia de los recursos públicos,** el uso de la tecnología en este punto es clave, dada la necesidad de contar con sistemas de información que permitan la optimización del proceso de control fiscal, que permitiría realizar las auditorias de manera remota, por medio del cual se minimizan gastos e incluso riesgos del personal en misión, toda vez que la información estaría disponible para el auditor en cualquier momento y en tiempo real, para lo cual es imprescindible la **seguridad de la información** que se maneje.

De igual forma, se podría pensar en la posibilidad de usar sistemas de información, que permitan la visibilidad del ejercicio auditor a través de sistemas en línea para seguimiento de la comunidad por medio de la pagina web, generando

confianza en la comunidad como resultado el ejercicio del control fiscal, de igual forma se pensaría en poder tener un sistemas de Peticiones Quejas y Reclamos efectivo que promueva la interacción de manera más ágil, y confiable, en el ejercicio de la participación ciudadana, lo que conlleva a la **transparencia, la eficacia y la eficiencia** de sus procesos.

Por su parte la estrategia Gobierno en Línea, como uno de sus componentes establece la determinación de un sistema de gestión de seguridad de la información, como un eje transversal en los procesos de toda organización publica de cualquier orden.

El siguiente es el nivel de madurez por dominio:

DOMINIOS	ACTUAL	ESPERADO
PLANEACIÓN Y DIRECCIÓN ESTRATÉGICA - PDE	**0,3**	**3**
GESTIÓN DE RIESGOS-RTI	**0,3**	**3**
GESTIÓN DE LA SEGURIDAD - GSI	**0,1**	**3**
GESTIÓN DE LA ARQUITECTURA EMPRESARIAL, ADQUISICIÓN Y SOPORTE- IAS	**0,1**	**3**
GESTIÓN DEL TALENTO HUMANO, APRENDIZAJE Y DESARROLLO - TAD	**0,5**	**3**
CONTROL, EVALUACIÓN Y MEJORA - CEM	**0,7**	**3**

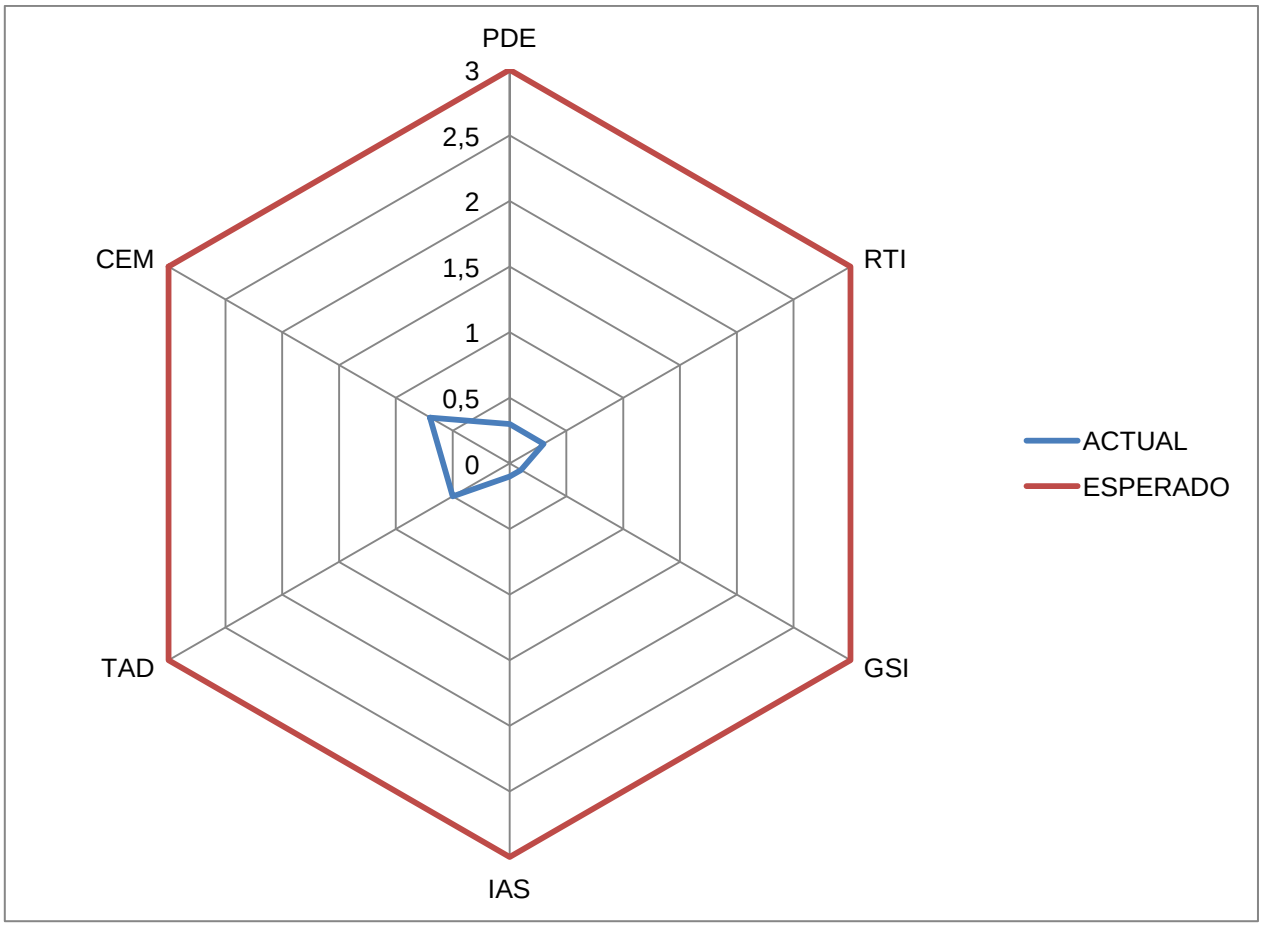


Grafico 2: Nivel de Madurez por dominio

Fuente: Elaboración propia

En ese orden de ideas, el dominio de Gestión de Seguridad de la Información (GSI) se encuentra en un nivel de madurez cero (0), y para lograr llevarlo al nivel tres (3), en el cual el proceso sea definido, ejecutado, implementado de forma gestionada, planificado, supervisado y ajustado, y sus resultados sean debidamente establecido, controlados y mantenidos, que es capaz de alcanzar sus objetivos.

13 PLAN DE IMPLEMENTACIÓN

Para lograr lo anterior, se determina el plan de implementación, en un plazo de tres años, en el cual se tendrán en cuenta los siguientes procesos:

PDE02 Esquema de Gobierno de TI

GSI01 Establecer y Documentar el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI)

GSI02 Supervisar y revisar el SGSI.

GSI03 Seguridad de los Recursos Humanos

GSI04 Gestión de Activos

GSI05 Control de Acceso

GSI06 Criptografía

GSI07 Gestión de la Seguridad Física y del Entorno

GSI08 Gestión de seguridad en las operaciones

GSI09 Gestión de seguridad de las Comunicaciones

IAS03 Gestionar la Continuidad

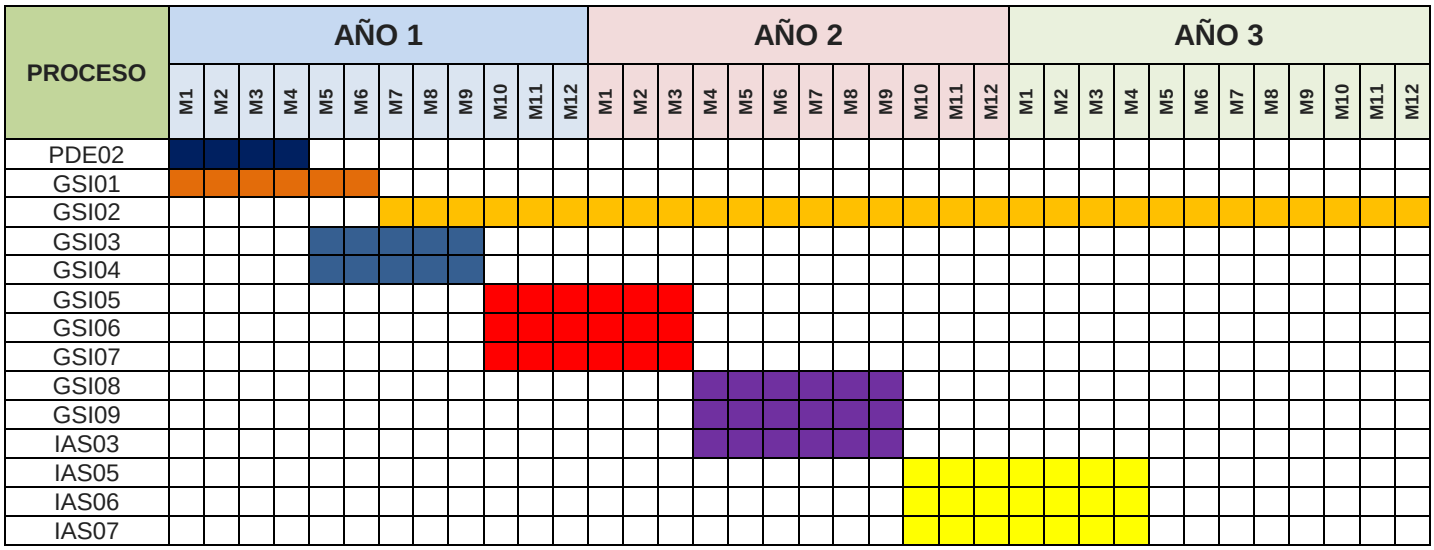
IAS05 Gestión de proveedores

IAS06 Gestión de Incidentes

IAS07 Gestión de seguridad en la adquisición, desarrollo y mantenimiento de sistemas

13.1 CRONOGRAMA

El siguiente cronograma muestra los procesos a implementar y su tiempo de ejecución estimado.



13.2 CARACTERIZACIÓN DE LOS PROCESOS

Proceso	Entradas	Salidas
PDE02 Esquema de Gobierno de TI	Sistema de gestión de Calidad. Políticas Institucionales. Estructura Organizacional.	Políticas De Gobierno y gestión de TI Documento caracterización de proceso Gestión de TI. Estructura de TI
Actividades		
PDE02.A01: Definir las políticas, lineamientos y directrices que hacen parte de la estrategia de Gobierno de TI, de acuerdo con las políticas institucionales de la entidad.		
PDE02.A02: Estructurar e implementar un macro-proceso de gestión de TI que permita direccionar, evaluar y monitorear las capacidades de TI, asegurando el adecuado aprovisionamiento del talento humano y los recursos necesarios para ofrecer los servicios de TI de la institución.		
PDE02.A03: Definir los roles y funciones en la estructura de TI, que tienen responsabilidades en la toma de decisiones de TI.		
Indicadores		
Nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa		
Número de roles de seguridad claves claramente definidos		
Porcentaje de procesos críticos, servicios TI y programas habilitados por las TI cubiertos por evaluaciones de riesgos.		

Proceso	Entradas	Salidas
GSI01: Establecer y Documentar el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI)	Diagnostico Organizacional. Políticas Institucionales. Estructura Organizacional.	Documento Sistema de Gestión de Seguridad de La Información. Documento políticas de Seguridad de la información. Plan de Comunicación del SGSI. Plan de Tratamiento de Riesgos de seguridad de la información.
Actividades		
GSI01.A01: Determinar las cuestiones Internas y externas que son pertinentes para los propósitos de la entidad y que afectan su capacidad para lograr los resultados del sistema.		
GSI01.A02: Determinar las necesidades y expectativas de la Partes Interesadas		
GSI01.A03: Determinar el Alcance del SGSI		
GSI01.A04: Alinear el SGSI con el enfoque global de la gestión de la seguridad en la empresa.		
GSI01.A05: Obtener autorización de la dirección para implementar y operar o cambiar el SGSI.		
GSI01.A06: Definir y documentar la Política de seguridad de la Información que sea adecuada al propósito de la organización, incluya objetivos de seguridad y el compromiso de la dirección para mantener y mejorar el SGSI.		
GSI01.A07: Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.		
GSI01.A08: Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. Asegurar que el plan identifica las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los riegos identificados de seguridad de información.		
Indicadores		
Nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa		
Número de roles de seguridad claves claramente definidos		
Porcentaje de procesos críticos, servicios TI y programas habilitados por las TI cubiertos por evaluaciones de riesgos.		

Proceso	Entradas	Salidas
GSI02: Supervisar y revisar el SGSI.	Documento Sistema de Gestión de Seguridad de La Información. Documento políticas de Seguridad de la información. Plan de Comunicación del SGSI. Plan de Tratamiento de Riesgos de seguridad de la información.	Plan de Auditorías Internas al SGSI. Formatos de medición del desempeño del SGSI. Plan de mejoramiento del SGSI.
Actividades		
GSI02.A01: Realizar revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y		

prácticas de seguridad del SGSI. Considerar los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas.
GSI02.A02: Realizar auditorías internas al SGSI a intervalos planificados.
GSI02.A03: Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.
GSI02.A04: Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.
GSI02.A05: Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.
Indicadores
Número de incidentes de seguridad causados por la no observancia del plan de seguridad
Porcentaje de cumplimiento de los controles del SGSI.
Número de incidentes relacionados con la seguridad.

Proceso	**Entradas**	**Salidas**
GSI03 Seguridad de los Recursos Humanos	Sistema de Gestión de Seguridad de La Información. Políticas de Seguridad de la información. Plan de vacantes. Plan de Capacitaciones. Manual de funciones y competencias laborales.	Formato de verificación de antecedentes. Acuerdos de confidencialidad. Plan de Inducción y Re inducción.
Actividades		
GSI03.A01: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.		
GSI03.A02: Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.		
GSI03.A03: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.		
GSI03.A04: Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.		
GSI03.A05: Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.		
GSI03.A06: Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.		
Indicadores		
Porcentaje de funcionarios que ingresan a quienes se les realiza verificación de antecedentes		
Nivel de funcionarios entrenados en las políticas de seguridad de la información de la empresa.		
Número de incidentes de seguridad causados por la no observancia del plan de seguridad.		

Proceso	Entradas	Salidas
GSI04 Gestión de Activos.	Sistema de Gestión de Seguridad de La Información. Políticas de Seguridad de la información. Inventario de almacén.	Inventario de Activos. Formato de entrega y devolución de activos. Procedimiento para la gestión de medios removibles.
Actividades		
GSI04.A01: Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.		
GSI04.A02: Los activos mantenidos en el inventario deben tener un propietario.		
GSI04.A03: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.		
GSI04.A04: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.		
GSI04.A05: Se debe desarrollar e implementar procedimientos un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.		
GSI04.A06: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización,		
GSI04.A07: Se deben implementar procedimientos para la gestión de medios removibles de acuerdo con el esquema de clasificación adoptado por la organización.		
GSI04.A08: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.		
GSI04.A09: Los medios que contienen información, se deben proteger contra accesos no autorizados, uso indebido o corrupción durante el transporte.		
Indicadores		
Numero de inventarios activos de información.		
Porcentaje de incidentes de seguridad registrados, relacionados con el uso de medios removibles.		
Número de incidentes de seguridad registrados, por el uso indebido de activos.		

Proceso	Entradas	Salidas
GSI05 Control de Acceso	Sistema de Gestión de Seguridad de La Información. Políticas de Seguridad de la información.	Políticas de Control de Acceso. Derechos de acceso de los usuarios aprobados. Política de gestión de contraseñas.
Actividades		
GSI05.A01: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.		
GSI05.A02: Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.		
GSI05.A03: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.		
GSI05.A04: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.		

GSI05.A05: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
GSI05.A06: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
GSI05.A07: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
GSI05.A08: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
GSI05.A09: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
GSI05.A10: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
GSI05.A11: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
GSI05.A12: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
GSI05.A13: Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
GSI05.A14: Se debe restringir el acceso a los códigos fuente de los programas.
Indicadores
Promedio de tiempo entre los cambios y actualizaciones de cuentas
Número de cuentas (con respecto al número de usuarios/empleados autorizados)
Número de incidentes relacionados con accesos no autorizados a la información

Proceso	Entradas	Salidas
GSI06 Criptografía.	Sistema de Gestión de Seguridad de La Información. Políticas de Seguridad de la información.	Políticas de Uso de Controles Criptográficos.
Actividades		
GSI06.A01: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.		
GSI06.A02: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.		
Indicadores		
Porcentaje de uso de controles criptográficos en el envío de información.		

Proceso	Entradas	Salidas
GSI07 Gestión de la Seguridad Física y del Entorno	Sistema de Gestión de Seguridad de La Información. Políticas de Seguridad de la información.	Procedimiento de seguridad física. Señalización de áreas seguras, restringidas o reservadas. Formato de préstamo de equipos informáticos. Política de escritorio limpio. Directrices de bloqueo de equipos de forma automática.
Actividades		
GSI07.A01: Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.		
GSI07.A02: Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.		
GSI07.A03: Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.		
GSI07.A04: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.		
GSI07.A05: Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.		
GSI07.A06: Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.		
GSI07.A07: Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.		
GSI07.A08: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.		
GSI07.A09: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información deben estar protegido contra interceptación, interferencia o daño.		
GSI07.A10: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.		
GSI07.A11: Los equipos, información o software no se deben retirar de su sitio sin autorización previa.		
GSI07.A12: Se debe aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.		
GSI07.A13: Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o rehusó.		
GSI07.A14: Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.		
GSI07.A15: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.		
Indicadores		
Porcentaje de áreas seguras delimitadas respecto de la cantidad de áreas seguras.		
Número de incidentes de seguridad registrados relacionados por accesos no autorizados.		
Número de incidentes presentados por personas no autorizadas.		

Proceso	Entradas	Salidas
GSI08 Gestión de seguridad en las operaciones	Sistema de Gestión de Seguridad de La Información. Políticas de Seguridad de la información. Manual de procesos y procedimientos. Plan de Auditorías Internas.	Formato de control de cambios. Procedimiento para la realización de copias de respaldo de la información y sistemas. Registros de actividades de los usuarios en los sistemas. Procedimiento para la instalación de software.
Actividades		
GSI08.A01: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.		
GSI08.A02: Se debe controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.		
GSI08.A03: Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.		
GSI08.A04: Se debe separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.		
GSI08.A05: Se debe implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.		
GSI08.A06: Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.		
GSI08.A07: Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.		
GSI08.A08: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.		
GSI08.A09: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.		
GSI08.A10: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.		
GSI08.A11: Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.		
GSI08.A12: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.		
GSI08.A13: Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.		
GSI08.A14: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se debe planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.		
Indicadores		
Porcentaje de individuos que reciben formación de concienciación relativa al uso de dispositivos de usuario final.		
Numero de códigos maliciosos detectados.		

Porcentaje de incidentes de seguridad relacionados con software malicioso.

Proceso	Entradas	Salidas
GSI09 Gestión de seguridad de las Comunicaciones	Sistema de Gestión de Seguridad de La Información. Políticas de Seguridad de la información. Políticas de Uso de Controles Criptográficos. Acuerdos de Confidencialidad	Políticas de transferencia de Información. Seguimiento a los acuerdo de confidencialidad. Directrices de separación de redes de información.
Actividades		
GSI09.A01: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.		
GSI09.A02: Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.		
GSI09.A03: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.		
GSI09.A04: Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.		
GSI09.A05: Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.		
GSI09.A06: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.		
GSI09.A07: Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.		
Indicadores		
Porcentaje de incidentes de seguridad relacionados con la divulgación de información no autorizada.		
Porcentaje de funcionarios con acuerdos de confidencialidad (en relación al total de funcionarios)		
Nivel de capacitación de usuarios en el manejo y divulgación de información sensible.		

Proceso	Entradas	Salidas
IAS03 Gestión de la Continuidad.	Sistema de Gestión de Seguridad de La Información. Manual de Procesos Y procedimientos. Estructura organizacional.	Plan de Continuidad.
Actividades		
IAS03.A01: Identificar los procesos empresariales internos y externalizados, y actividades de servicio que son críticos para las operaciones de la empresa o necesario para cumplir obligaciones legales y / o contractuales, así mismo lo requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas.		
IAS03.A02: Definir y documentar los objetivos y el alcance mínimo acordado de la política de		

continuidad del negocio y la necesidad de integrar la planificación de la continuidad en la cultura de la empresa.
IAS03.A03: Definir y documentar un plan de continuidad que contemple los activos críticos, el análisis de impacto (BIA), tiempos mínimos de recuperación, duración aceptable y duración máxima de recuperación, requerimientos, recursos y responsables de los activos de información.
IAS03.A04: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa,
Indicadores
Porcentaje de servicios TI que cumplen los requisitos de tiempos de funcionamiento
Porcentaje de restauraciones satisfactorias y en tiempo de copias alternativas o de respaldo
Porcentaje de medios de respaldo transferidos y almacenados de forma Segura
Número de sistemas críticos para el negocio no cubiertos por el plan
Número de ejercicios y pruebas que han conseguido los objetivos de recuperación
Porcentaje de interesados internos y externos que han recibido formación

Proceso	Entradas	Salidas
IAS05 Gestión de proveedores	Sistema de Gestión de Seguridad de La Información. Manual de Contratación.	Acuerdos de Niveles de servicios – ANS Formato de Seguimiento a los proveedores.
Actividades		
IAS05.A01: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización.		
IAS05.A02: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso.		
IAS05.A03: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información.		
IAS05.A04: Se debe hacer seguimiento y auditar con regularidad la prestación de servicios de los proveedores.		
IAS05.A05: Se deben gestionar los cambios en el suministro de servicios, por parte de los proveedores, incluido el mantenimiento y las mejoras de la política, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta a criticidad de la información, sistemas y procesos del negocio involucrado y la reevaluación de los riesgos.		
Indicadores		
Porcentaje de proveedores que cumplen con los requisitos acordados		
Número de infracciones de servicio causadas por los proveedores		
Numero de reuniones de revisión con proveedores		

Proceso	Entradas	Salidas
IAS06 Gestión de Incidentes	Sistema de Gestión de Seguridad de La Información. Plan de Continuidad.	Procedimiento de atención de incidentes de seguridad de la información. Registro de incidentes de seguridad de la información.
Actividades		

IAS06.A01: Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
IAS06.A02: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
IAS06.A03: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
IAS06.A04: Los eventos de seguridad de la información se debe evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
IAS06.A05: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
IAS06.A06: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.
IAS06.A07: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
Indicadores
Número y porcentaje de incidentes que causan interrupción en los procesos críticos de negocio
Tiempo promedio entre incidentes de acuerdo con el servicio facilitado por TI.
Nivel de satisfacción del usuario con la resolución de las peticiones de servicio.
Tiempo promedio transcurrido para el tratamiento de cada tipo de petición de servicio
Porcentaje de incidentes resueltos dentro de un periodo acordado/aceptable

Proceso	Entradas	Salidas
IAS07 Gestión de seguridad en la adquisición, desarrollo y mantenimiento de sistemas	Sistema de Gestión de Seguridad de La Información. Plan de Continuidad.	Requisitos de seguridad de la información para el desarrollo de sistemas. Procedimiento para la adquisición de sistemas de información.
Actividades		
IAS07.A01: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.		
IAS07.A02: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.		
IAS07.A03: La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.		
IAS07.A04: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.		
IAS07.A05: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.		
IAS07.A06: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.		
IAS07.A07: Se deben desalentar las modificaciones a los paquetes de software, que se deben		

limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
IAS07.A08: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
IAS07.A09: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
IAS07.A10: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
IAS07.A11: Durante el desarrollo se debe llevar a cabo pruebas de funcionalidad de la seguridad.
IAS07.A12: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se debe establecer programas de prueba para aceptación y criterios de aceptación relacionados.
IAS07.A13: Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.
Indicadores
Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados.
Porcentaje de incidentes de servicios registrados, relacionados con la gestión de requerimientos de los sistemas.
Número de errores encontrados durante las pruebas
Porcentaje de productos recibidos que cumplen con los requisitos establecidos.

CONCLUSIONES Y RECOMENDACIONES

Una vez abordada la literatura del marco teórico y referencial, se evidencia la necesidad de contar con un gobierno corporativo organizado, con una estructura de decisión clara y que direccione de forma asertiva la visión estratégica de la empresa, con el fin de poder hacer frente a los cambios del entorno en el cual está inmerso, como parte de ese entorno se resaltan las tecnologías de la información y la comunicación, que se han constituido en parte importante en el desarrollo de las organizaciones.

En relación a lo anterior, se le da importancia al gobierno de TI como el centro de coordinación para una gestión más eficaz, alrededor de temas importantes, como la alineación, el liderazgo, la planificación, la ejecución, la rendición de cuentas, la gestión del cambio, los indicadores clave de rendimiento y temas relacionados, a los cuales TI hace soporte o apalanca de algún modo.

De igual forma, el gobierno de TI garantiza que los objetivos de TI estén alineados con la estrategia de la empresa y le permite administrar sus recursos, gestionar los riesgos, la seguridad de la información, además del desempeño de sus recursos para generar valor agregado a la empresa.

Lo definido en el acápite anterior, aplica tanto para las empresas privadas, como las públicas, grupo del cual hacen parte las Contralorías territoriales, quienes deben hacer frente en un entorno global que cambia rápidamente y de forma dinámica alrededor de cuestiones como la innovación, el cumplimientos de leyes y regulaciones, la rendición de cuentas más eficaz, la globalización, tecnologías más sofisticadas, entre otros.

En relación al gobierno de TI, se observó la poca inmersión de las contralorías en este concepto, por lo cual este proyecto nos llevó a la definición del framework de Gobierno y gestión de TI en estas entidades, con el fin de contar con una herramienta que apoye la consecución de los objetivos de TI, mas allá de ser considerados un

soporte insustancial, a ser una propuesta de valor estratégica, para la consecución de los objetivos corporativos, además de lograr el cumplimiento de la normatividad legal aplicable a la entidades del sector público en Colombia, tales como la estrategia Gobierno en Línea, la protección y privacidad de datos personales, entre otras.

Dicho framework, vincula un marco de trabajo como COBIT 5, que ha sido validado en distintas empresas del sector público y privado, para el gobierno y la gestión de TI, en alianza con normas tales como ISO 27001 e ISO 31000, quienes convergen en un solo modelo propuesto para las Contralorías Territoriales.

Para lograr lo antepuesto, se realizó un mapeo entre las mejores prácticas de COBIT 5 e ISO/IEC 27001 ajustables al framework propuesto para gestionar la seguridad de la información de la Contraloría General del Departamento de La Guajira, en el cual se denota que varios de los procesos de COBIT se encuentran contenidos en la norma ISO, lo que llevo a la definición de procesos ajustados al caso de estudio, sin embargo, pueden ser aplicados también a las demás entidades similares.

Por otra parte, se adopta el proceso de gestión Riesgos basado en la Norma ISO/IEC 31000, propicio para la identificación, valoración y tratamiento de los riesgos asociados a TI, el cual puede ser aplicado de forma transversal a toda la organización, en cada uno de los procesos que esta gestiona a través de su sistema integrado de gestión.

Una vez definido el marco de trabajo aplicable a las contralorías, se propuso identificar el nivel de madurez actual, en este caso de la Contraloría General del Departamento de La Guajira, en cuanto a gobierno, gestión y seguridad de la información, resultó en que esta entidad se encuentra en un nivel inmaduro respecto a los procesos del modelo propuesto, por debilidades, tanto de orden administrativo como financiero, sin embargo también existen algunas fortalezas y oportunidades que bien podrían apoyar la implementación de un buen esquema de gobierno de TI y gestionar de forma correcta la seguridad de la información.

Con el fin de lograr este propósito, se propuso un plan de implementación enmarcado en la Seguridad de la Información, para la Contraloría General del Departamento de La Guajira, el cual contempla la definición de los procesos, actividades y requisitos necesarios para su ejecución, medición y seguimiento, de manera progresiva, los cuales contribuirán a la generación de valor de TI en la entidad.

Para el caso de la aplicación de un modelo de gobierno y gestión en las contralorías territoriales, es recomendable hacer un análisis del contexto organizacional, la alta dirección debe estar interesada en promover estas buenas prácticas y se debe contar con un equipo de trabajo que responda a la ejecución de este proyecto de manera efectiva, buscando el acompañamiento de toda la organización sobre todo del recurso humano, que es importante para el éxito de lo encomendado.

Para terminar, es importante dar el primer paso, no será algo sencillo, se tendrán obstáculos que puedan afectar el desarrollo del proyecto de implementación, sin embargo, es pertinente contar con una buena planeación que permita mantener el rumbo e ir poco a poco logrando grandes cambios en las entidades, para este caso en la Contraloría General del Departamento de La Guajira.

REFERENCIAS BIBLIOGRÁFICAS

Contraloría General del Departamento de La Guajira. (2016). PLAN ESTRATÉGICO 2016-2019.

Selig, G. (2010) Implementing IT Governance

Norfolk, David. (2011) IT Governance.

Ladino, M. I., Villa, P. A., & María, A. L. E. (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. Scientia Et Technica, 1(47), 334-339.

Salazar Saavedra, C. A., & Vela Londoño, E. (2012). Gobierno de TI en Colombia. Documentación y modelado de procesos que soportan el Gobierno y la Gestión de las Tecnologías de Información (TI).

Arora, V. (2010). Comparing different information security standards: COBIT vs. ISO 27001. Línea. Disponible en Carnegie Mellon University, Qatar:(http://qatar. cmu. edu/media/assets/CPUCIS2010-1. pdf).

Ministerio de Tecnologías de la información y la comunicación - MINTIC. (2016). MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Línea. Disponible en http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html.

Muñoz Serna, R., & Martínez Arias, M. A. (2012). Caracterización de procesos de gestión de TI basados en COBIT 5 y mapeo con ISO27002, ITIL, CMMI DEV, PMBOK, para la implementación en la industria editorial colombiana, apoyando el proceso de transformación digital.

Carpio, G.M., & Camargo, M. S. (2011). Diseño de una Metodología para la implementación de un Marco de Gobierno de TI en las Pymes Colombianas basado en COBIT 4.1.

Banco Mundial. (2005). Foro Mundial sobre Gobierno Corporativo - Guía del Usuario. Washington, D.C.

BITCompany. (2015). CobiT: Un marco de referencia para la información y la tecnología. Retrieved June 7, 2017, from http://www.bitcompany.biz/que-es-cobit/#.WTrG7mg1-ks

Consulting, P. (2015). GC-web. Retrieved May 5, 2017, from http://www.partnerconsulting.com.pe/web/index.php?option=com_content&task=view&id=119&Itemid=9

ICAEW. (n.d.). The Hampel Report. Retrieved May 28, 2017, from http://www.icaew.com/en/library/subject-gateways/corporate-governance/codes-and-reports/hampel-report

ISACA. (2012). Cobit 5: Un marco de negocio para el Gobierno y la Gestión de la Empresa.

ISO. (2013). ISO/IEC 27002:2013. Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información. Retrieved June 8, 2017, from https://www.iso.org/standard/54533.html

Laudon, F., & Laudon, J. (1996). Sistemas de Información. Editorial Diana, México. Retrieved from http://www.academia.edu/download/35209817/Sistemas_Informacion.docx

López Neira, A., & Ruiz Spohr, J. (2005). ISO 27000.es. Retrieved June 8, 2017, from http://www.iso27000.es/iso27000.html

MinTic, M. de T. de la I. y las C. (2015). Estrategia Gobierno en Línea. Retrieved June 22, 2017, from http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-14714.html

MINTIC, M. de T. de la I. y las C. (2015). Manual Estrategia de Gobierno en Línea. Retrieved from http://estrategia.gobiernoenlinea.gov.co

Network Sec. (2013). Implantación de Gobierno de TI (Tecnologías de la Información), 17. Retrieved from http://www.network-sec.com/gobierno-TI/implantacion-IT-governance

Organización para la Cooperación y el Desarrollo Económico (OCDE). (2004). Principios de Gobierno Corporativo de la OCDE. Ocde, 67. https://doi.org/10.1787/9788485482726-es

Superintendencia financiera de Colombia. (2010). Documento conceptual de gobierno corporativo, 21. Retrieved from https://www.superfinanciera.gov.co/SFCant/GobiernoCorporativo/doccongb200810pub.pdf

Trasobares, A. H. (2003). Los sistemas de información: evolución y desarrollo. Proyecto Social: Revista de Relaciones Laborales, (10), 149–165.

Weill, P., & Jeanne W. Ross. (2004). IT Governance: how top performers manage IT decision rights for superior results. Bostos, Massachusetts: Harvard Bussines School Press.

Williams, R. W. (1998). Corporate Governance Report: From Greenbury To Hampel — A Mid-Term Report On Developments In Directors' Remuneration. Corporate Governance: An International Review, 6(2), 123–124. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=10452253&site=ehost-live&scope=site

IT Governance Institute. (2010) Gobierno de las TIC ISO/IEC 38500. [En línea]. http://www.isaca.org/Journal/JOnline/Pages/default.aspx,

ANEXOS

ANEXO 1: FICHA TÉCNICA ENCUESTA GOBIERNO Y GESTIÓN DE TI- CONTRALORÍAS TERRITORIALES

*Obligatorio

1. Dirección de correo electrónico *

2. Nombre entidad *

3. Nivel Territorial *

- ○ Departamental Distrital Municipal

GESTIÓN ESTRATÉGICA DE TI

4. La entidad tiene un área de gestión de TI

- ○ Si
- ○ No

5. El área de TI pertenece al nivel

- ○ Estratégico
- ○ De apoyo a la gestión

6. La entidad cuenta con un funcionario Líder del área de TI (Director - coordinador)

- ○ Si
- ○ No

7. La persona Responsable del área de TI es de nivel

- ○ Asesor
- ○ Directivo
- ○ Profesional
- ○ Técnico
- ○ Asistencial

8. La entidad tiene definido dentro del plan estratégico 2016 - 2019, el componente de gestión estratégica de TI.

- ○ Sí
- ○ No
- ○ Aun en Construcción

9. La entidad tiene definido el Plan estratégico de TI (PETI), para la vigencia 2016 - 2019

- ○ Sí
- ○ No
- ○ En Construcción

10. La institución cuenta con una definición de Arquitectura Empresarial que aplique el Marco de Referencia de Arquitectura Empresarial para la gestión de TI del país

- ○ Sí
- ○ No
- ○ En construcción

11. La dirección de TI o quien haga sus veces tiene identificados y definidas las políticas y estándares que faciliten la gestión y la gobernabilidad de TI, contemplando por lo menos los siguientes temas (seleccione los que correspondan):

Selecciona todos los que correspondan.

- ○ Seguridad de la Información
- ○ Continuidad del negocio
- ○ Gestión de información
- ○ Adquisición tecnológica
- ○ Desarrollo e implantación de sistemas de información
- ○ Acceso a la tecnología y uso de las facilidades por parte de los usuarios
- ○ Ninguno

12. La dirección de TI o quien haga sus veces tiene definidos e implementa el plan de comunicación de la estrategia, las políticas, los proyectos, los resultados y los servicios de TI.

- ○ Si
- ○ No
- ○ En construcción

GOBIERNO DE TI

13. La dirección de TI o quien haga sus veces tiene definido e implementa un esquema de Gobierno TI alineado con la estrategia misional y con el Modelo Integrado de Planeación y Gestión, que estructure y direccione el flujo de las decisiones de TI

- ○ Sí
- ○ No

14. La dirección de TI o quien haga sus veces apoya la especificación de las necesidades de sistematización y demás apoyo tecnológico requerido por los procesos de la institución, de tal manera que se incorporan facilidades tecnológicas que contribuyan a mejorar la articulación, calidad, eficiencia, seguridad y reducir los costos de operación.

- ○ Si
- ○ No

15. La dirección de TI o quien haga sus veces tiene estructurado e implementado un macro- proceso de gestión de TI, según los lineamientos del Modelo Integrado de Planeación y Gestión de la institución que incorpore metas e indicadores.

- ○ Sí
- ○ No
- ○ En construcción

16. La dirección de TI o quien haga sus veces genera, direcciona, evalúa y monitorea las capacidades de TI , asegurando el adecuado aprovisionamiento del

talento humano y los recursos necesarios para ofrecer los servicios de TI de la institución.

○ Si

○ No

17. La entidad realiza las compras de bienes o servicios de Tecnología a través de Acuerdos Marco de Precios (AMP) existentes, en caso de que apliquen, y da prioridad a adquisiciones en modalidad de servicio o por demanda, Además propender por minimizar la compra de bienes de hardware.

○ Si

○ No

18. La Dirección de TI o quien haga sus veces define los criterios y metodologías que direccionen la toma de decisiones de inversión en Tecnologías de la Información (TI), buscando el beneficio económico y de servicio de la institución.

○ Si

○ No

19. La dirección de TI o quien haga sus veces lidera la planeación, ejecución y seguimiento a los proyectos de TI.

○ Si

○ No

20. La dirección de TI o quien haga sus veces, realiza el monitoreo y evaluación de desempeño de la gestión de TI a partir de las mediciones de los indicadores del macro- proceso de Gestión TI

- ○ Si
- ○ No
- ○ No existe el Macro-proceso de gestión de TI

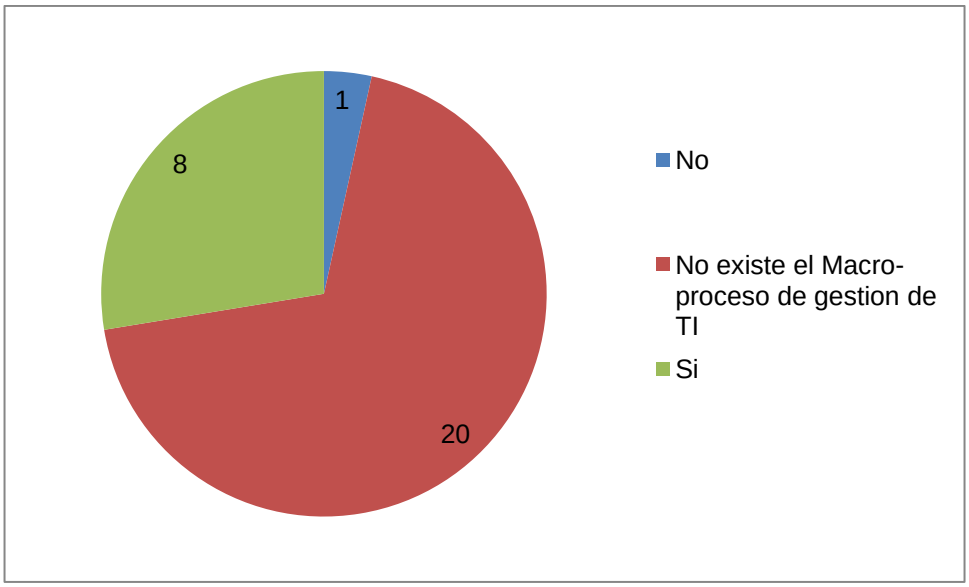
ANEXO 2: RESPUESTAS ENCUESTA GOBIERNO Y GESTIÓN DE TI, CONTRALORÍAS TERRITORIALES.

Ver, Archivo De Excel

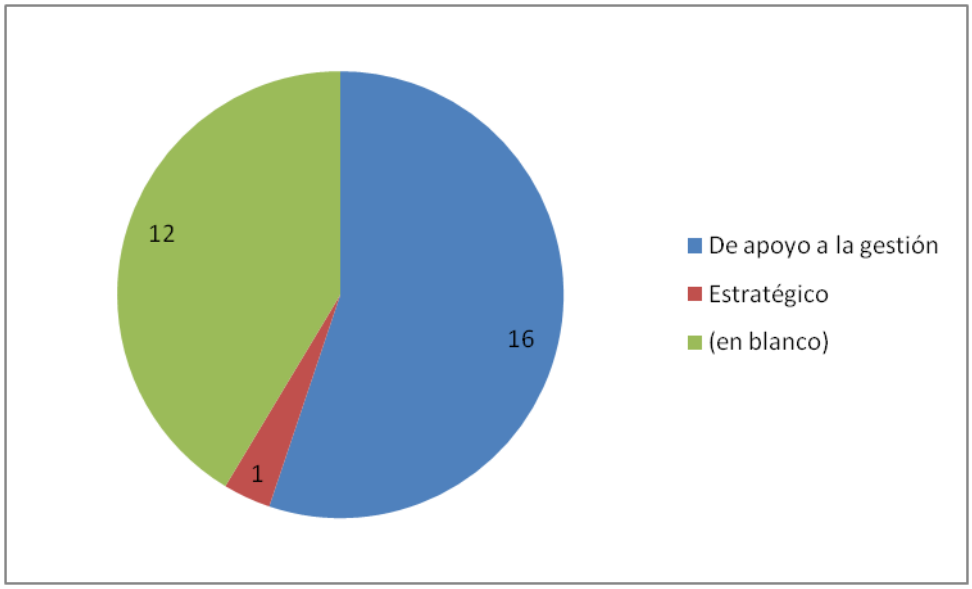
ANEXO 3: GRÁFICOS DE CONSOLIDADOS DE RESPUESTAS.

GESTIÓN ESTRATÉGICA DE TI

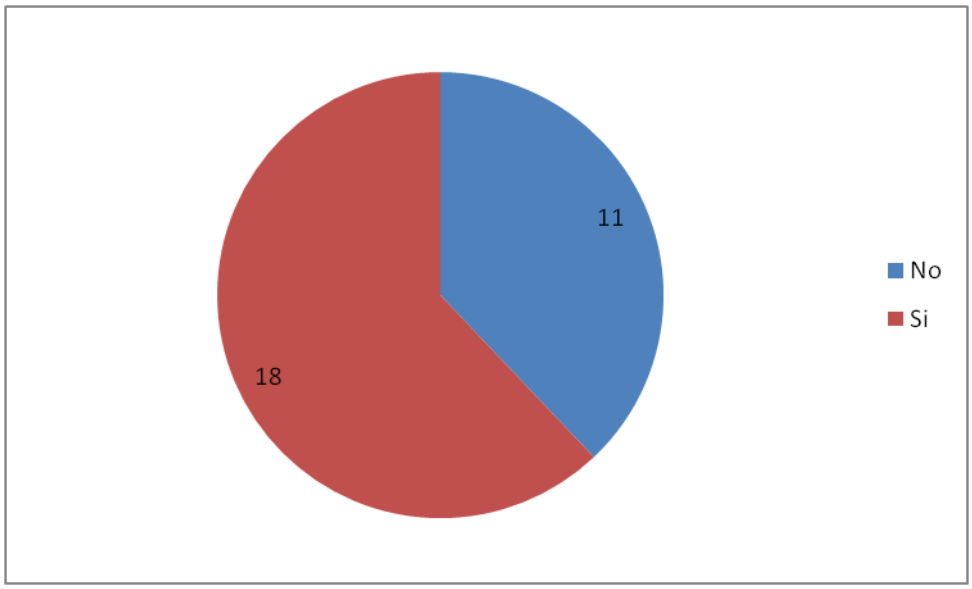
4. La entidad tiene un área de gestión de TI



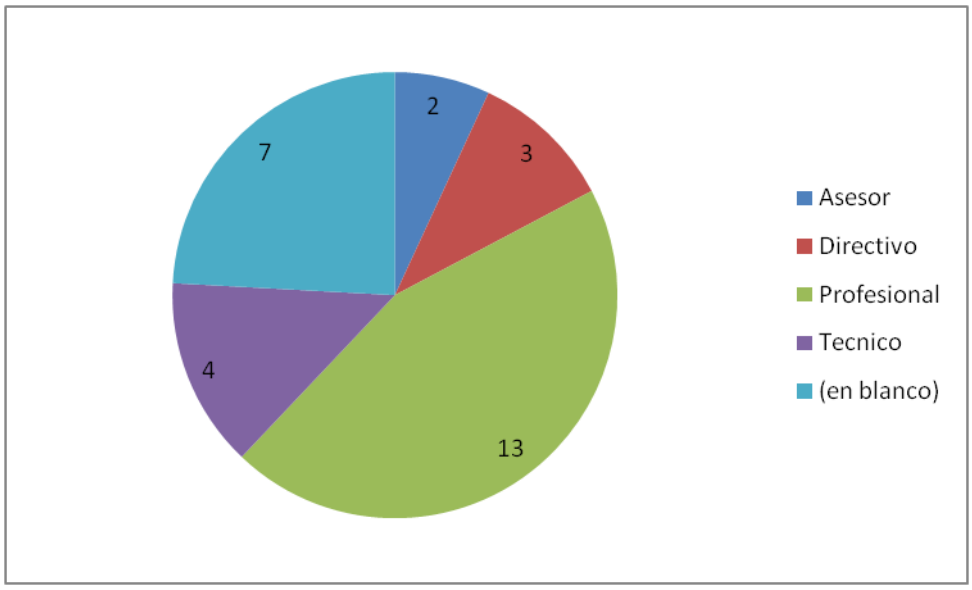
5. El área de TI pertenece al nivel



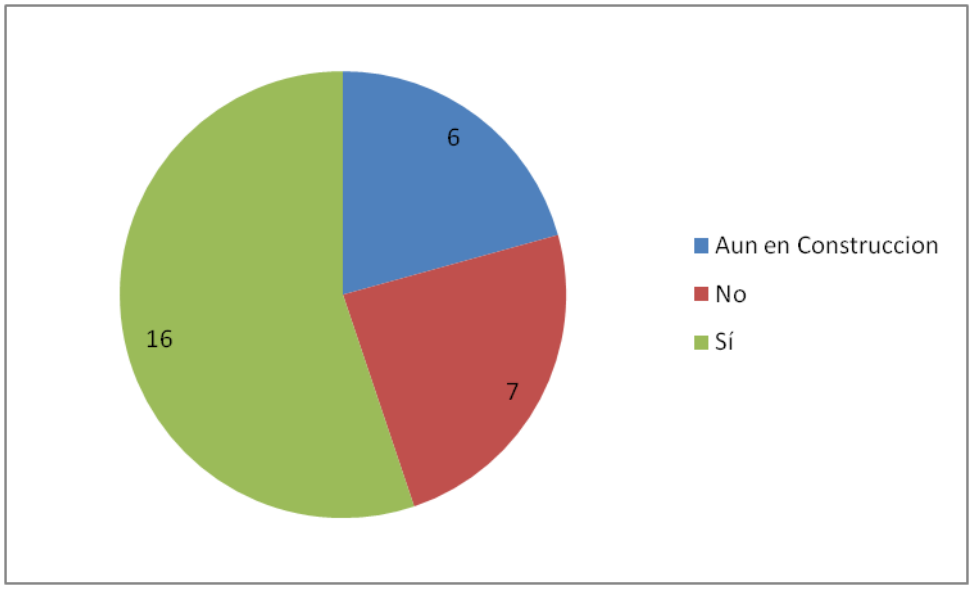
6. La entidad cuenta con un funcionario Líder del área de TI (Director - coordinador)



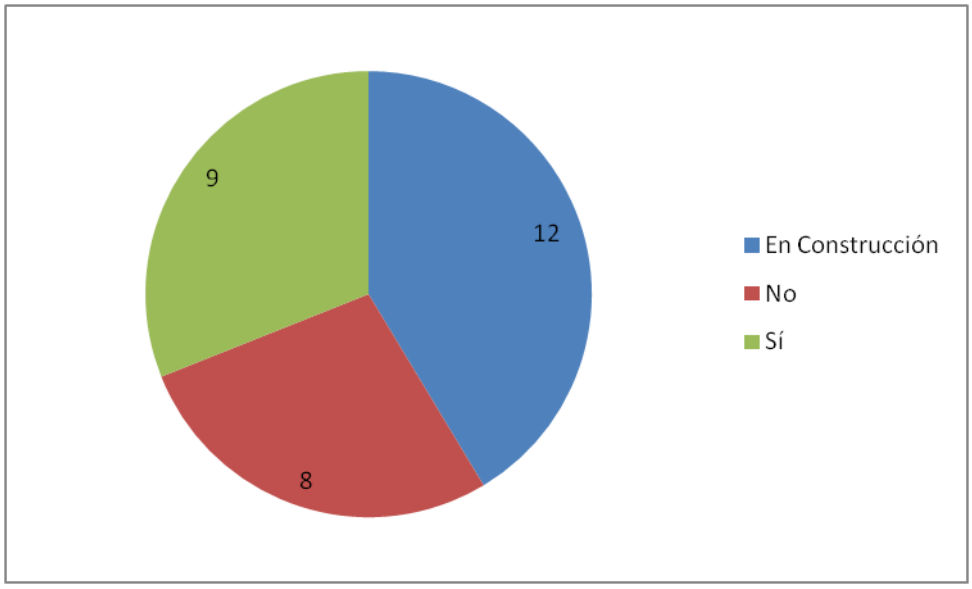
7. La persona Responsable del área de TI es de nivel



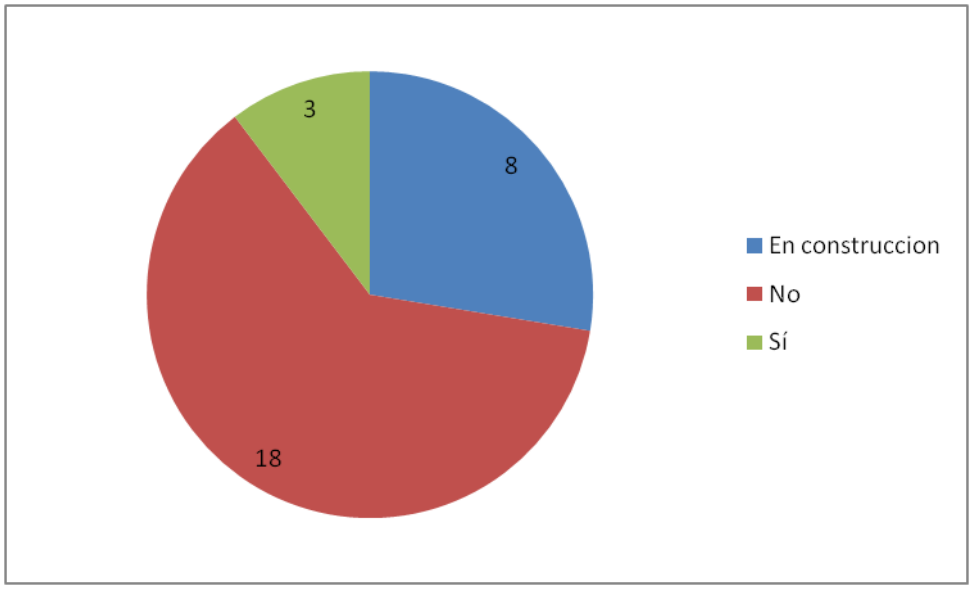
8. La entidad tiene definido dentro del plan estratégico 2016 - 2019, el componente de gestión estratégica de TI.



9. La entidad tiene definido el Plan estratégico de TI (PETI), para la vigencia 2016 – 2019



10. La institución cuenta con una definición de Arquitectura Empresarial que aplique el Marco de Referencia de Arquitectura Empresarial para la gestión de TI del país.

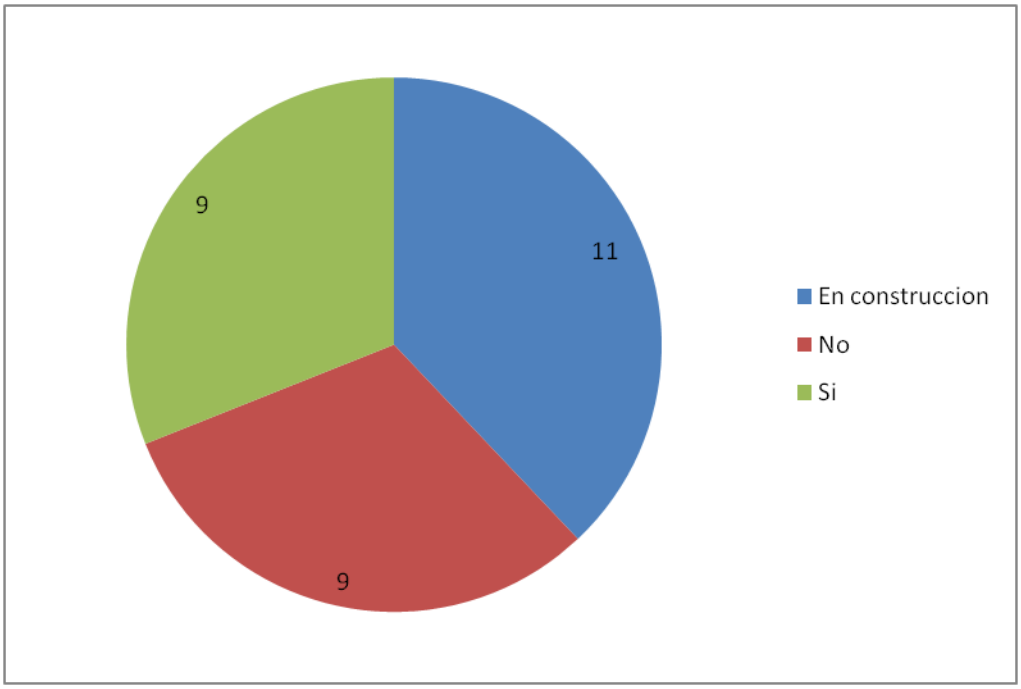


11. La dirección de TI o quien haga sus veces tiene identificados y definidas las políticas y estándares que faciliten la gestión y la gobernabilidad de TI, contemplando por lo menos los siguientes temas (seleccione los que correspondan).

Adquisición tecnológica, Acceso a la tecnología y uso de las facilidades por parte de los usuarios
Continuidad del negocio, Acceso a la tecnología y uso de las facilidades por parte de los usuarios
Continuidad del negocio, Adquisición tecnológica, Acceso a la tecnología y uso de las facilidades por parte de los usuarios
Gestión de información, Adquisición tecnológica, Desarrollo e implantación de sistemas de información
Gestión de información, Desarrollo e implantación de sistemas de información
Ninguno
Seguridad de la Información
Seguridad de la Información, Adquisición tecnológica
Seguridad de la Información, Continuidad del negocio, Acceso a la tecnología y uso de las facilidades por parte de los usuarios
Seguridad de la Información, Continuidad del negocio, Gestión de información, Acceso a la tecnología y uso de las facilidades por parte de los usuarios
Seguridad de la Información, Continuidad del negocio, Gestión de información, Adquisición tecnológica, Acceso a la tecnología y uso de las facilidades por parte de los usuarios
Seguridad de la Información, Continuidad del negocio, Gestión de información, Adquisición tecnológica, Desarrollo e implantación de sistemas de información
Seguridad de la Información, Continuidad del negocio, Gestión de información, Adquisición tecnológica, Desarrollo e implantación de sistemas de información, Acceso a la tecnología y uso de las facilidades por parte de los usuarios
Seguridad de la Información, Gestión de información, Adquisición tecnológica

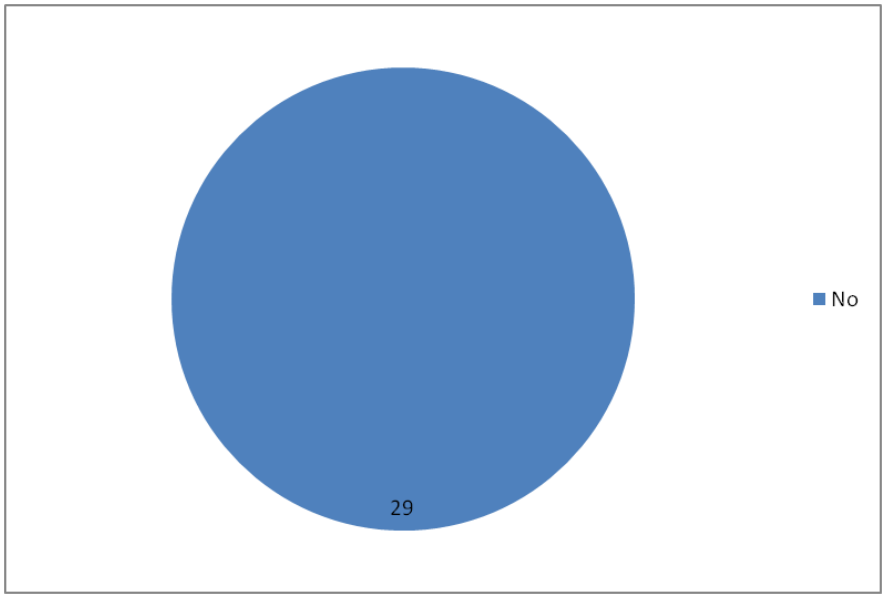
Seguridad de la Información, Gestión de información, Adquisición tecnológica, Acceso a la tecnología y uso de las facilidades por parte de los usuarios
Seguridad de la Información, Gestión de información, Adquisición tecnológica, Desarrollo e implantación de sistemas de información, Acceso a la tecnología y uso de las facilidades por parte de los usuarios

12. La dirección de TI o quien haga sus veces tiene definidos e implementa el plan de comunicación de la estrategia, las políticas, los proyectos, los resultados y los servicios de TI.

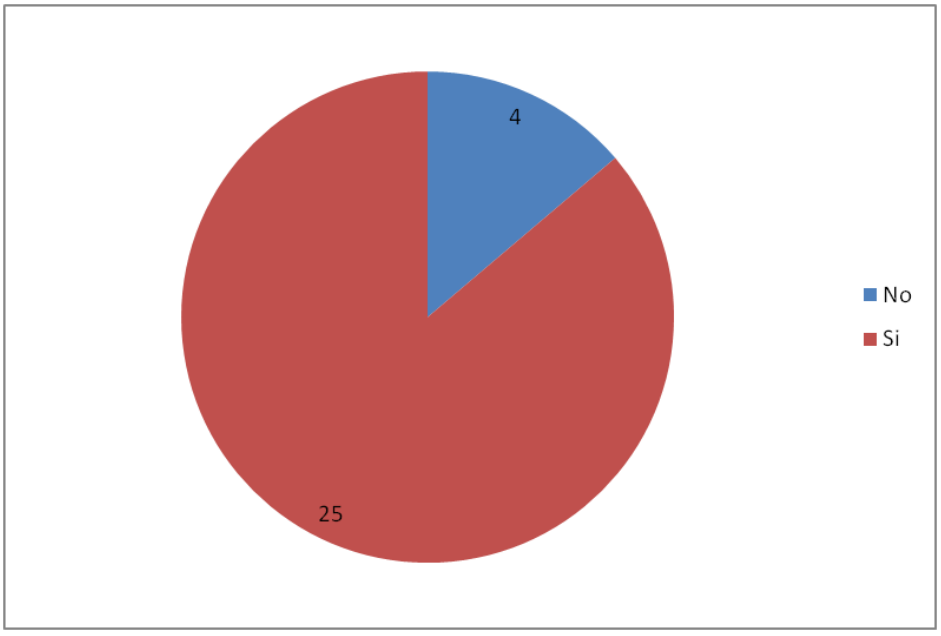


GOBIERNO DE TI

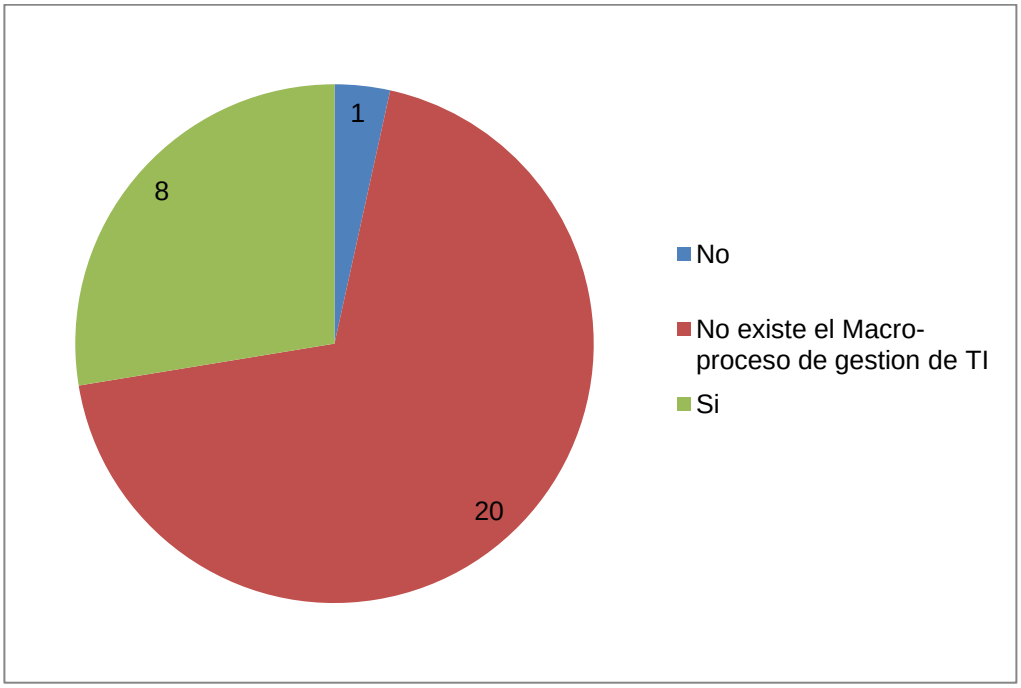
13. La dirección de TI o quien haga sus veces tiene definido e implementa un esquema de Gobierno TI alineado con la estrategia misional y con el Modelo Integrado de Planeación y Gestión, que estructure y direccione el flujo de las decisiones de TI



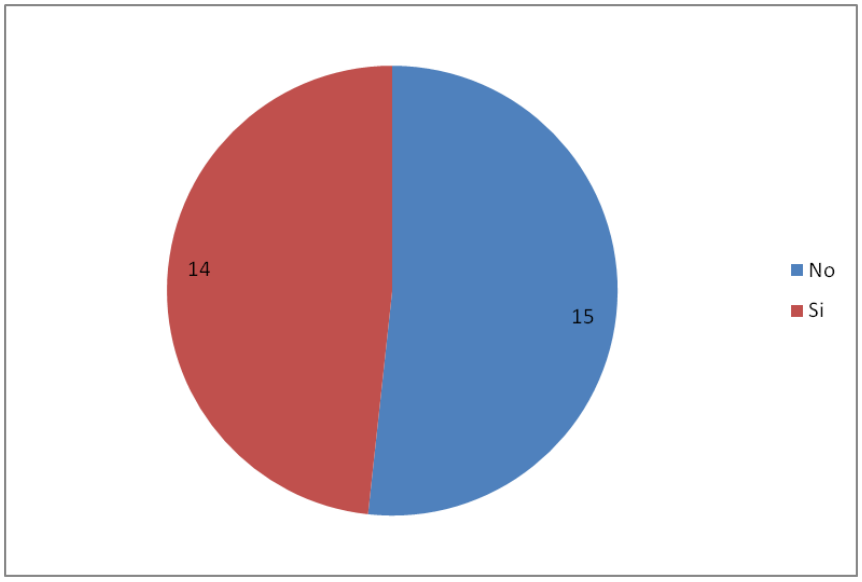
14. La dirección de TI o quien haga sus veces apoya la especificación de las necesidades de sistematización y demás apoyo tecnológico requerido por los procesos de la institución, de tal manera que se incorporan facilidades tecnológicas que contribuyan a mejorar la articulación, calidad, eficiencia, seguridad y reducir los costos de operación.



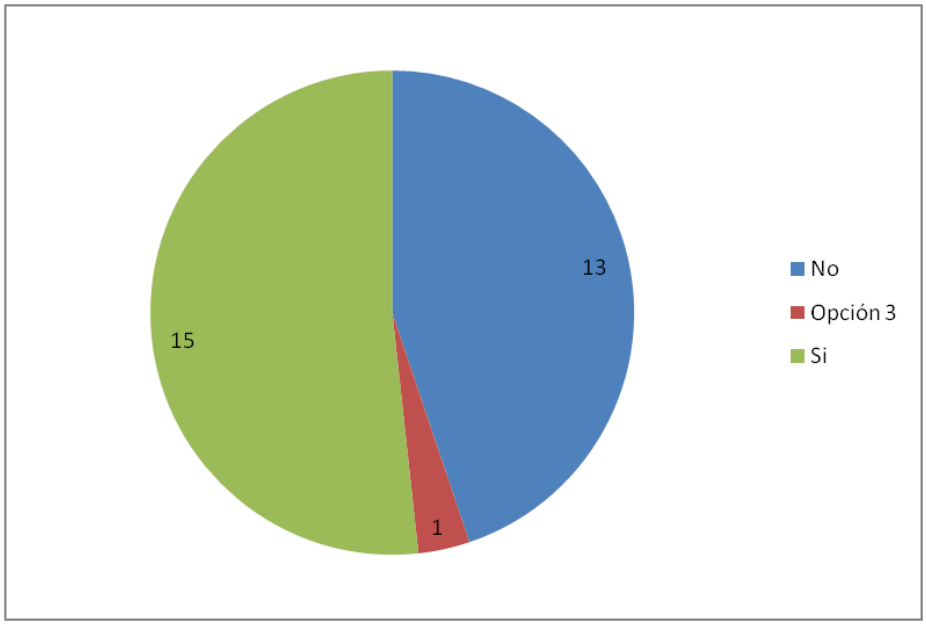
15. La dirección de TI o quien haga sus veces tiene estructurado e implementado un macro- proceso de gestión de TI, según los lineamientos del Modelo Integrado de Planeación y Gestión de la institución que incorpore metas e indicadores.



16. La dirección de TI o quien haga sus veces genera, direcciona, evalúa y monitorea las capacidades de TI, asegurando el adecuado aprovisionamiento del talento humano y los recursos necesarios para ofrecer los servicios de TI de la institución.

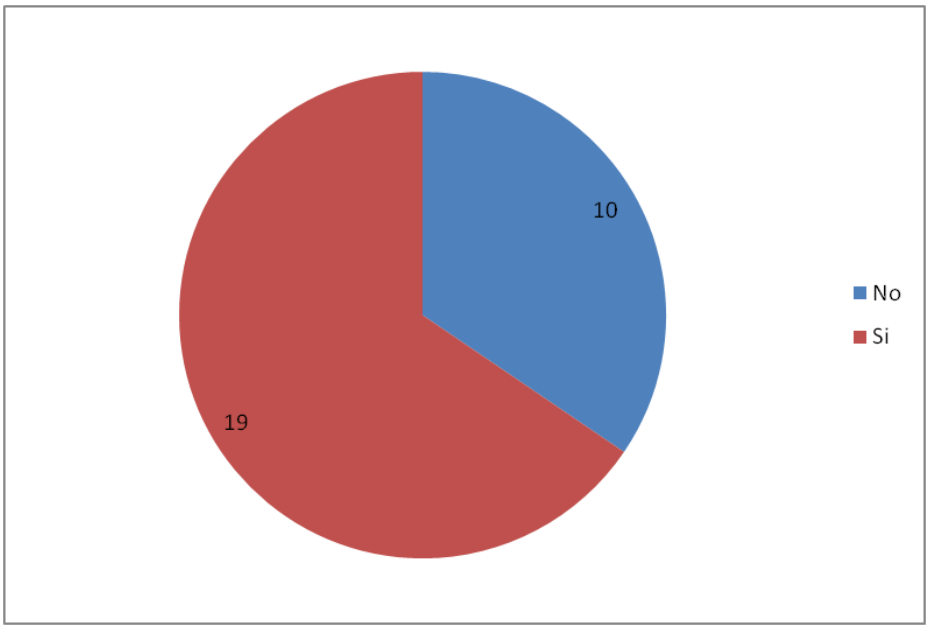


17. La entidad realiza las compras de bienes o servicios de Tecnología a través de Acuerdos Marco de Precios (AMP) existentes, en caso de que apliquen, y da prioridad a adquisiciones en modalidad de servicio o por demanda, Además propender por minimizar la compra de bienes de hardware.

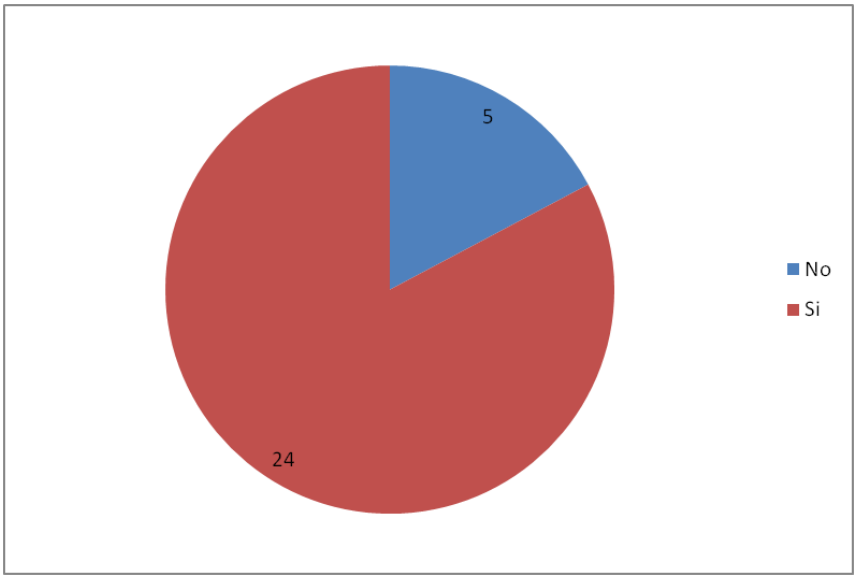


18. La Dirección de TI o quien haga sus veces define los criterios y metodologías que direccionen la toma de decisiones de inversión en Tecnologías de la

Información (TI), buscando el beneficio económico y de servicio de la institución.



19. La dirección de TI o quien haga sus veces lidera la planeación, ejecución y seguimiento a los proyectos de TI.



20. La dirección de TI o quien haga sus veces, realiza el monitoreo y evaluación de desempeño de la gestión de TI a partir de las mediciones de los indicadores del macro- proceso de Gestión TI